Security in IoT Networks

Kumar Prasun (2422CS12) , Mehar Keshvendra Singh (2422CS07)

April 24, 2025

Abstract

The expansion of IoT and its billions of connected embedded devices has raised many security challenges. The focus of this paper is providing an overview of the security in the IoT architecture as well as addressing how the multi-class multi-layer attack surface is formed across IoT networks. Tracing the current **threat landscape** - featuring key attacks and vulnerabilities – along with highlighting fundamental security challenges arising from device constraints, heterogeneity, and scale. Describe common attack vectors, review defense mechanisms, and define best practices for mitigating IoT threats. Insecure IoT deployments can cause real-world **case studies** (like the Mirai botnet, a smart aquarium breach). We survey important standards and frameworks (including the NIST guidance and the ETSI EN303645) that aim to foster improvements to IoT security and novel emerging technologies that are likely to increase protections going forward, like machine learning and blockchain. Finally, we provide insights into future research directions for constructing security-aware IoT networks. This paper provides insights on the status of IoT security and the way forwards.

1 Introduction

The *Internet of Things* (IoT) is the internetworking of physical devices ("things"), including unique identifiers (UIDs) and embedded computing systems that enable these objects to collect and exchange data. The Internet of Things (IoT) has seen explosive growth in the last few years, with applications that encompass everything from smart homes and wearables to industrial control systems and smart cities. The active number of IoT devices worldwide was about 14.3 billion in 2022 and is expected to be around 16.7 billion in 2023[3] This staggering scope underscores the revolutionary power of IoT across sectors but also the pressing need for security. In fact, IoT devices are become *prime targets* for cyber attackers. In 2023, an industry report commented that IoT devices were the most targeted asset type, overtaking traditional computers and mobile device. Several high-profile incidents have shown that compromises of IoT systems can lead to significant, harmful effects, from massive collapses of the Internet to the disclosure of sensitive data.

IoT deployments are often recognised as heterogeneous and resource-constrained while being deployed in different environments, which is in contrast to traditional

IT systems. Many IoT devices do not have user management or monitoring interfaces, so traditional security controls are difficult (or impossible) to implement. Moreover, the IoT devices are often in use beyond the secure enterprise perimeters (for instance, in homes and public spaces), rendering them viable targets for physical tampering and a plethora of other threats. All of these factors add up to a **"perfect storm" of security challenges**: a dramatically expanded attack surface, numerous soft targets, and frequently underwhelming defense measures. Consequently, attackers have taken advantage of IoT vulnerabilities to create botnets, surveil users, and break into networks through these otherwise innocuous things (e.g., thermostats, cameras, or lightbulbs).

We bring up a detail investigation on the security concerns in the IoT networks. We first discuss the common multiple layers of the IoT architecture and some of the security implications at each layer. We then outline the present **threat landscape**, in which we enumerate the topologies of attacks recorded against IoT platforms. Then, we examine major **security challenges** specific to IoT, including device constraints and absence of standardisation. We investigate prevalent **attack vectors** an adversary employs to compromise IoT devices and networks. In the **defence mechanisms** section, we review existing techniques and best practices for securing IoT devices and networks, including device hardening and network monitoring. We present **case studies** on significant IoT security incidents for practical takeaways. Additionally, we survey key **standards and frameworks** that have emerged to help manufacturers, developers, and deployers alike build on IoT security. We also outline new technologies, such as machine learning-driven anomaly detection and blockchain, that can strengthen IoT security. Lastly, we identify **future research directions** to tackle the key open issues and end with our insights on securing the next generation of IoT networks.

2 IoT Architecture

Layers are commonly used to describe the **architectures** of IoT systems, dividing functionality into multiple abstraction levels.

An introductory model is the *three-layer architecture*:

- **Perception Layer**: Comprises the physical devices (sensors and actuators) that perceive or act upon the environment.
- **Network Layer**: Enables connectivity (e.g., via protocols such as Wi-Fi, Zigbee, Bluetooth, LTE, etc.) by transferring data from the devices to back-end systems.
- **Application Layer**: Consists of software services and consumer-facing applications that process IoT data and provide interfaces to users.

Many sources expand this into four- or five-layer models by adding intermediate layers:

- *Four-layer architecture*: Adds a **processing/support layer** (typically executed through edge or cloud computing) between the network and application layers to enable data aggregation, analytics, and device management.
- *Five-layer architecture*: Further adds a **business layer** on top, providing high-level business processes and advanced analytics to extract insights from IoT data.

These architecture models are illustrated in Figure 1.

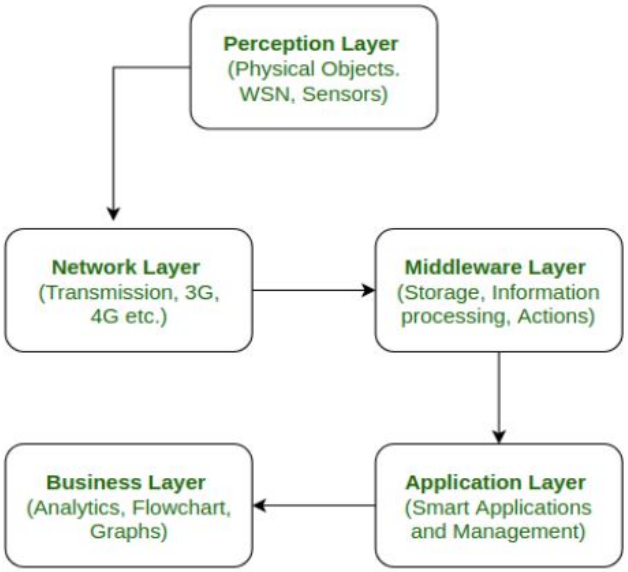

Figure 1: Common IoT architectures illustrating three, four, and five layers (Perception, Network, Support/Processing, Application, and Business) [**?**]. Each additional layer (from 3 to 5) offers specialised capabilities but also brings additional security considerations.

The IoT architecture has different security concerns and attack surfaces for each layer:

- **Device/Perception Layer:** IoT devices are often low-powered in terms of computing and memory resources; therefore, heavyweight security functions—such as strong encryption or complex intrusion detection—may not be feasible on these devices. Many sensors and embedded systems lack a user interface and are frequently shipped with default credentials or hard-coded keys, which are rarely changed. Physical security is a major concern at this layer, as devices are often deployed in unsecured environments where attackers may have physical access to modify hardware or extract firmware. Additionally, ensuring data authenticity and confidentiality from the point of

capture is a critical challenge, as data without source authentication, integrity verification, and encryption cannot be trusted.

- **Network layer:** This layer is the communication channels (e.g. local networks, gateways, Internet) that connect IoT devices to servers or to each other. Major security problems consist of eavesdropping, man-in-the-middle attacks, and routing attacks. Most IoT protocols are wireless (Wi-Fi, Bluetooth, Zigbee, etc) which, by design, makes it possible to spy on or jam communications. The variety of network protocols also introduces a patchwork of security standards – some IoT-specific protocols have historically shipped without encryption or strong authentication by default, for example. Segurely adding devices to netvorks (i.e.,initial authehtication aend key exchange). The network-layer devices themselves such as IoT gateways or routers must also be secured as they aggregate connectivity for multiple endpoints.

- **Application/Cloud Layer** — Where IoT data usually lands into an applications or enterprise systems in cloud storage to be stored, analyzed and further taking action. At this layer, typical application security threats are relevant, such as securing databases of sensor data, implementing access controls that limit which users or devices are allowed to access certain information or commands, and preventing injection attacks on interfaces (e.g., insecure APIs or web frontends for IoT device management). Privacy also plays a big role at the application layer, as IoT commonly gathers sensitive personal or operational information.

These layers do not exist in vacuums either, as cross-cutting concerns such as **identity management**,**encryption key management** and **update mechanisms** traverse the entire architecture. The weakness within one layer could be the weakness of the entire system – the attacker, if compromises a device (perception layer) vulnerability, can laterally move to the network layer to reach the cloud servers. Hence, IoT architecture design must be based on a holistic, layered security approach ("defense in depth").

3 Threat Landscape

The IoT threat landscape has rapidly expanded in conjunction with IoT adoption. Early IoT deployments often prioritized functionality over security, which attackers have been quick to capitalize on. Today, IoT threats range from large-scale network disruptions to targeted attacks on specific devices or data. We outline some prominent categories of threats observed:

Botnets and Distributed Denial of Service (DDoS): Perhaps the most infamous IoT threat to date is the use of compromised IoT devices to form botnets that launch DDoS attacks. A landmark example is the *Mirai* botnet in 2016, where

malware infected hundreds of thousands of IoT devices (CCTV cameras, home routers, etc.) by exploiting default passwords. The Mirai botnet was then used to flood major Internet services with traffic, exceeding 1 Tbps in attack magnitude. This massive DDoS crippled several high-profile targets – including the servers of DNS provider Dyn, which in turn caused outages at popular websites[2]. Mirai demonstrated that IoT botnets can leverage sheer numbers to disrupt critical Internet infrastructure. Since Mirai's source code was released publicly, numerous variants and copycat IoT malwares have appeared, keeping large-scale DDoS a persistent threat.

Unauthorized Access and Device Takeover: Many IoT devices have been hijacked by attackers to either join botnets or perform malicious actions (like spying or sabotage). Weak authentication is a common culprit. For instance, devices protected only by factory-default login credentials (e.g., "admin/admin") can be easily discovered and accessed by attackers – a tactic Mirai automated by scanning for devices and attempting a small dictionary of common passwords[1]. In other cases, firmware vulnerabilities allow remote code execution on devices. Once an attacker gains control of a device, they can often pivot deeper into the network or exploit the device's functionality (e.g., disable an alarm system, or use an IP camera to surveil a home). Insecure interfaces in the IoT ecosystem (mobile apps, cloud dashboards, etc.) have also been abused to gain unauthorized access to devices and data.

Data Breaches and Privacy Threats: IoT deployments collect extensive data, some of it sensitive (e.g., health data from wearables, or video from home cameras). This makes IoT data stores an attractive target for hackers. Breaches can occur if communications are not encrypted or if cloud databases are left unsecured. Attackers have intercepted unencrypted sensor data or commands in transit, compromising confidentiality and sometimes even manipulating messages (integrity attacks). A dramatic example involved a casino that was hacked through an Internet-connected fish tank thermometer: attackers exploited the vulnerable thermostat to gain a foothold in the casino's network, then accessed a high-roller database and exfiltrated it through the thermostat's connection. This incident highlights how even innocuous IoT devices can serve as backdoors to valuable data. Privacy is also at risk when IoT devices (like smart assistants or cameras) are commandeered to surveil users.

Threats to Safety-Critical Systems: As IoT integrates with physical systems (industrial control, automotive, healthcare), cyber attacks can have kinetic consequences. Compromises of Industrial IoT (IIoT) or Industrial Control Systems (ICS) devices can disrupt production lines or critical infrastructure. For example, an attack on a smart HVAC or smart grid controller could cause physical damage or unsafe conditions. In the automotive realm, researchers have demonstrated remote attacks on connected cars, raising the specter of malicious actors harming passengers by manipulating vehicles. These high-stakes scenarios significantly elevate the importance of IoT security in certain domains.

Overall, the threat landscape for IoT is diverse and evolving. Attackers range from opportunistic botnet herders exploiting easy targets, to sophisticated adver-

saries targeting IoT as a stepping stone into corporate networks or as a means to cause physical disruption. Notably, many IoT attacks leverage the scale of insecure deployments: a single weak device might seem minor, but in aggregate such devices can facilitate widespread attacks. Defensive strategies must therefore address both individual device security and systemic risks posed by large fleets of IoT nodes.

4 Security Challenges in IoT

The challenges of securing IoT networks are unique and arise from the characteristics of IoT devices and the environments in which they are deployed. We address some of the keyoposition challenges below:

Resource Constraint: The IoT devices are generally designed to be economic, small, and energy-efficient. They often have a small processing power, memory, and energy availability (in particular for battery-powered or energy harvesting sensors). This greatly restricts what types of security features can be embedded in physical devices. But strong encryption and authentication protocols, for example, can be CPU- or memory-heavy for a tiny microcontroller. More sophisticated security functionalities such as intrusion detection agents or blockchain clients might be simply impossible to run. The challenge becomes devising *lightweight* security solutions that will operate within these restrictions, or forgoing security on the device itself, instead delegating it to gateways or cloud services, at the cost of exposing the device.

Scale and Manageability: The volume of IoT devices deployed (potentially tens or hundreds of thousands in a single organization) makes security hard to manage. Traditional IT security assumes regular patching, monitoring, and maintenance, whereas many IoT devices lack automated update mechanisms or, at least, the capacity to be easily patched. Even as vulnerabilities are discovered, many (if not most) IoT devices run in the field for years without any updates. Bad news for administrators: monitoring an extensive inventory of disparate devices that have varying firmware and capabilities is challenging; such visibility and control gaps form blind spots for attackers to exploit. The enlarged **attack surface** — every machine is a potential backdoor — requires defenders to protect and watch over an utterly unprecedented array of endpoints. "There's just a lot of IoT," as one cybersecurity expert put it. It increases the attack surface and much of this is not addressed by traditional defenses.

Heterogeneity and Standardization Gaps: In IoT, we see heterogeneous platforms, operating systems (most devices run dedicated real-time OS or firmware), and communication protocols. In contrast to the relatively homogeneous world of PCs or smartphones, IoT has no one-size-fits-all set of standards. It causes problems of interoperability and inconsistent security postures. Ultimately, some devices may use proprietary protocols with undocumented security properties. Notably, there has historically been no single, common set of security standards that

all IoT manufacturers adhere to. The result is extreme variation in security quality: one vendor's smart bulb may use strong encryption and authentication, while another's may be talking in plaintext with a default password. The industry's disjointed nature also leads security improvements to trickle out slowly; there are guidelines and best practices but they're not adopted uniformly.

Safety and Longevity of Devices: IoT devices have a longer and less attended lifecycle than personal computing devices. After installation (as with, say, a smart thermostat, or, say, a sensor embedded within concrete), an IoT device might run for a decade or longer with little to no further human engagement. The long-term security of such devices is difficult to guarantee. In the long run, cryptographic algorithms that are currently strong may become weak, certificates may expire and new threats may arise — but the device to be protected may no longer receive updates to handle those issues. Legacy IoT devices that have long been unsupported by manufacturers also represent a security risk, but these can be hard to replace if they are deeply embedded in operations.

Manufacturer Security Practices: The IoT market's rapid innovation and cost reduction has led to security being an afterthought for many manufacturers. Indeed, vendors are noted to often spend extensive resources on adding features and other easy to use functions to gain market share while *overlooking security actions* leading to devices that are " routinely being hacked" This is often due to poor practices, such as hard-coded or universal default passwords, lack of secure boot mechanisms and little to no security testing. We also saw some manufacturers not establish a process for vulnerability disclosure and patching. The upshot is a deluge of insecure gadgets on the market. And while this is beginning to change (squeezed by regulation and consumer demand for security), legacy devices will be around for a while.

Privacy and Data Protection: IoT devices gather extensive data, possibly including people's personal lives (fitness trackers, smart home devices) or delicate industrial operations. Securing this data against unauthorised access remains a challenge in the areas of both security and privacy. Compliance with privacy regulations (such as GDPR) can be challenging when data is stored and processed across many devices and cloud services. We must also figure out how to allow users some control over their data relating to IoT devices and implement data minimisation (that is, only collecting what needs to be collected when it comes to devices). If data is not properly secured, there can be privacy openings even in well-meaning IoT implementations — including when data leaks or is misused.

Physical and Environmental Challenges: Many IoT devices function in uncontrolled or hostile environments, including outdoor sensors exposed to the elements, wearable or implantable devices inside of humans or animals, and devices in remote or otherwise hard-to-access locations. This makes them more susceptible to physical tampering (an attacker may physically reset a device to factory settings to take advantage of default creds, or interface directly with hardware debug ports). It can also complicate routine maintenance (such as firmware updates) if devices are not easily reachable. Attackers have the chance to steal devices and

reverse-engineer them to discover vulnerabilities at their convenience.

To summarise, IoT security has to deal with constraints and circumstances not found in classical IT. Any comprehensive IoT security strategy must take these challenges into account — and overcome them, whether through employing lightweight cryptography or building better device management tools, creating incentives for manufacturers to do so or developing for IoT what most guidebooks might refer to as the new return of secure by design standards that create coherence around the IoT ecosystem's security posture.

5 Common Attack Vectors

To defend against attacks, we must first understand how they occur in IoT systems – the **attack vectors**. We go through some of the most common path attackers take to compromise IoT devices and networks:

- **Weak or Default Credentials:** In fact, the majority of IoT breaches start from devices secured with factory-default usernames/passwords or other weak credentials. Attackers frequently query the internet for IoT devices (for example, by querying common IP ranges or utilizing engines like Shodan) then to try to log in with known default passwords (for instance: admin", password") or easy to guess passwords. The Mirai malware, in particular, relied on a short list of around 60 common credentials to quickly brute-force devices. Since many users never modify the default login, this simple technique can gain access to thousands of hardware. Similarly, hardcoded credentials or backdoor accounts left by manufacturers also provide an easy entry point if discovered. The solution is simple: IoT devices should not have a default credential at all and enforce strong, unique passwords or some other form of authentication.

- **Unpatched Vulnerabilities:** IoT devices generally use firmware with known SW vulnerabilities (e.g., legacy Linux kernels, old libraries) that attackerscan exploit remotely. For example, an arbitrary code execution can be triggered bya stack-based buffer overflow in the targeting device's web interface or left-open debugging service. Attackers often reverse engineer firmware on devices (obtained from devices or vendor sites) to discover vulnerabilities. Once a vulnerability is discovered, any device running that firmware is potentially vulnerable at scale if it is not patched. The second compounding factor is the lack of timely updates — the state of many devices in the field remain unpatched, even after a vendor eventually does release a patch, for a long time. IoT malware has been spread by attackers exploiting such gaps. One common trend involves moving laterally, i.e taking control of one compromised device and using it to probe the local network for additional vulnerable devices. It is vital to keep IoT software up to date and to build devices that can be securely updated remotely.

- **Insecure Network Services and APIs:** IoT device network services (e.g., HTTP/HTTPS servers to serve a web dashboard, Telnet/SSH for remote management, and ports for custom protocol to connect mobile apps) If such services are not properly secured, they can become entry points. For instance, an IoT camera may have an open Telnet service with the default password, or an API endpoint that is not properly authenticated. Attacks found here include those against insecure cloud or mobile interfaces(e.g., an IoT cloud service that fails to verify the identity of the device or utilizes weak tokens), which can allow attackers to execute commands on devices or access data. Attackers also seek out unintended exposures, like debug interfaces that are left open by accident. Aren't most IoT devices for network services (e.g. NTP,DNS)? To mitigate your attack surface when it comes to IoT it's important to disable any unnecessary services and apply the principle of least privilege to any interface that connects to the network.

- **Lack of Encryption (Data in Transit and at Rest):** When IoT communications do not use encryption attackers can sniff network traffic and steal sensitive data such as sensor readings or credentials. Wireless IoT protocols are especially vulnerable to eavesdropping if they are not encrypted (for example, some early smart home devices communicated in plaintext). Likewise, if a device has logged data or credentials to flash memory without encrypting it then a physical thief could extract this data. Insecure data transfer and storage is indeed the second of eight IoT vulnerabilities listed. Missing authentication may also enable man-in-the-middle attacks — an attacker could impersonate an authentic gateway or cloud server to which the device connects. So employing something such as TLS/DTLS to communicate over, and encryption (when supported by hardware) to encrypt sensitive storage on devices are your best two defences.

- **Physical Tampering and Side-Channel Attacks:** Physical access to an IoT device opens up the attacker to many hardware attacks. They may recover the firmware by accessing debugging interfaces (like UART or JTAG) or by directly dumping memory devices; this can lead to the extraction of cryptographic keys or sensitive sources. Alternatively, they might attempt to glitch, or fault-inject the device (e.g., by using voltage, or clock-manipulation), to circumvent security checking. It is possible, albeit sophisticated, to perform side-channel attacks, such as measuring power consumption in an attempt to pull the crypto key from a smart card or IoT crypto chip. While these attacks are hardware-centric, they require close proximity and are therefore relevant to devices that are in public or unprotected spaces. These vectors can be mitigated through physical hardening measures (tamper-evident seals, disabling debug interfaces, secure enclaves for key storage, etc.).

- **Social Engineering and User Interaction:** While many IoT devices are designed to work unattended, some are used directly (or indirectly) by human

users. On the user side, attackers may try to trick users into misconfiguring their devices or inappropriately installing malicious companion applications. Phishing attacks may focus on IoT system admins to obtain credentials followed by managing a collective of devices. For example, in a smart home scenario, an attacker could trick the user into installing a fake firmware update that was sent to him via email. So user awareness and secure update mechanisms (for example, signed firmware from trusted sources) also need to be considered.

In general, this means that there are diverse attack vectors here, taking advantage of not only technical vulnerabilities, but also poor configurations or systems and human-factor weaknesses. Thus an enterprise IoT defense strategy must therefore be holistic, which means adopters of IoMT must be vigilant over all the above vectors: kill default passwords, plug known bugs, harden every interface, enforce encryption, protect physical devices and educate users. This is then followed by the defense section presenting methods and mechanisms that can help us secure IoT networks against those threats.

6 Defense Mechanisms

Securing IoT networks requires a combination of **preventive**, **detective**, and **reactive** measures, applied at multiple layers from the device hardware up to the cloud. We discuss important defense mechanisms and best practices below:

Secure Device Hardware and Boot: From the device level,implementation of effective security begins. Hardware-based securityfeatures provide a root of trust. For instance, we can note thatmany of the modern IoT chipsets already have Trusted Execution Environment or a secure element that can store cryptographic keys securely and perform sensitive operations in isolation. **Secure boot** is an important mechanism whereby the firmware on the device is cryptographically signed by the manufacturer, and the device will only run code if it passes signature verification. This is to stop persistent malware from living through a reboot and to verify that the device isn't operating on tampered firmware. As an additional layer, some systems implement a **chain-of-trust** that spans from the bootloader into the OS to application code. Physical protections like tamper-resistant packaging, sensors that detect when the device is opened, or epoxying critical chips can discourage casual tampering.

Strong Authentication and Access Control: Here are some of the best IoT securitypractices. Basic password entry is frequentlyinadequate. Instead, you should only allowunique credentials per device (no shared defaults) and, if possible, stronger factors like certificate-based authentication or hardware tokens. Mutual authentication is best: a user or server should not just authenticate a device's identity, but thedevice should also authenticate that it is talking to a legitimate server (spoofing). TLS clientcertificates or a per-device pre-shared key can also be used for protocols like MQTT or CoAP. Role-based access control can be used to

ensure that even within an IoT system, each component has no more access than is necessary — e.g., a smart lightbulb would only accept commands from one specific hub, and the hub in turn would only accept firmware updates from a central server, etc. In an enterprise, network access control would allow IoT devices to live in a quarantined segment of the network until they successfully authenticate and attest to compliance (think an IoT-specific NAC solution).

Encryption of Data in Transit and at Rest: Sensitive data transfers via IoT must all be encrypted to modern standards (TLS/DTLS, IPsec, etc. for network traffic and application layer encryption for protocols that need it). This makes eavesdropping and tampering impossible. Reduced encryption protocols have appeared for constrained devices (the TLS/DTLS handshake can for instance be optimized with pre-shared keys to mitigate the need for costly public-key operations). Encryption can protect data at rest on devices or gateways against exposure in case a device is stolen. Secure key management is critical – keys can be provisioned at manufacturing (where secure key injection processes must be employed) or securely generated on device (via a hardware random number generator). Novel **lightweight cryptography** algorithms (such as some chosen by NIST's lightweight cryptography project) aim to achieve the same levels of encryption/authentication strength but with significantly less computational burden, making them ideal for IoT.

Secure Communication Protocols and Network Segmentation: IoT systems should use secure forms ofcommunication protocols in addition to basic encryption. To improve security, use HTTPS or MQTTS (MQTT over TLS)instead of plaintext HTTP/MQTT. With native IoT protocols, such as a **CoAP** (Constrained Application Protocol), and its secure counterpart, the **CoAPS** (CoAP over DTLS), it isalso possible. In a similar way, Zigbee is supporting AES encryption for confidentiality. VPNs or secure tunnels can be used deploy secure connections wherever appropriate between external IoT deployments and core networks. Network segmentation is an important measure to take: IoT devices should be segmented, or isolated, in their own subnet or VLAN, away from critical IT assets. In the case of an IoT device being compromised, segmentation can contain the attack's spread. Micro-segmentation can provide even more granular controls, and software-defined networking (SDN) can adapt network paths in real-time in accordance with device trust levels.

Intrusion Detection and Anomaly Monitoring: Since it is not possible to block all attacks, it is important to monitor IoT environments for suspicious activity. Conventional intrusion detection systems (IDS) can also be adapted to IoT networks, searching for signatures of known IoT malware or anomalous traffic patterns (for example, a normally quiet sensor suddenly floods networked with huge amounts of data which may imply compromise). Gateway network-based IDS/IPS can detect threats in IoT traffic . Anomaly detection techniques are also being applied more and more, as by baselining normal behavior of IoT devices (the norm usage of the network of an IoT device, the commands that it responds to, the timing of such commands, etc.), machine learning models can detect deviations from

normal behavior that could signal whether an attack is being attempted or that a malfunction is taking place. For example, an IoT thermostat that usually sends small data packets once a minute might be flagged if it suddenly starts sending large bursts of traffic at irregular intervals (perhaps exfiltrating data or taking part in a DDoS). Machine learning-based anomaly detection is known to increase IoT attack detection rates by a large percentage through some research. "The trade-off probably is between minimizing false positives and the systems getting thin on the ground and predicting too much with too little data from devices," he said. Since IoT devices themselves may not support host-based IDS, it is common to monitor network / cloud level.

Secure Lifecycle Management (Provisioning, Updates, Decommissioning): A full-spectrum defense needs to governIoT device security over its lifetime. When provisioning (that is, onboarding a new device), secure bootstrap procedures (for example, the **EAP-TLS** or **DPP (Device Provisioning Protocol)** can be established to securely connect a new device to the network and load keys. Secure over-the-air OTA updates- are needed for the updates. Updates should be signed by the vendor, sent over encrypted channels and, ideally, initiated or approved in a controlled manner. A few other IoT platforms are also using periodic check-in, in which each IoT device queries a secure server for updates. And of course the absence of any update mechanism (or an insecure one) renders devices forever vulnerable — hence "Lack of Secure Update Mechanism" is one of the most common vulnerabilities cited by OWASP[2]. On devices at the end of life, resource decommissioning — ensuring any sensitive data is wiped and cryptographic keys are revoked so a device that winds up in the bin can't be re-used later to get back into the network — should also be in place.

Network Access Control and Zero Trust Architecture: Enforcing a **Zero Trust** security model in and around the IoT devices can very effectively harden the environment. Zero Trust principles tell us that no device or node is trusted automatically, even when it is inside the network perimeter, and that all must be authenticated continuously. This means for IoT devices that each must be continually authenticated, authorized for every session or operation, and its behavior consistently assessed. Micro-segmentation (discussed above) is a component of Zero Trust – to restrict lateral movement. In some cases, organizations deploy dedicated **IoT security gateways** that serve as intermediaries for device communications, enforcing the policies (e.g., a surveillance camera may be allowed to send its video feed to the cloud storage service, but nowhere else). In case of a device goes rogue or is not compliant (for example, an appliance running on an out of date firmware), the gateway can quarantine the device.

Device Identity and Inventory Management: The first key pillar of an IoT cybersecurity strategy is to maintain an up to date inventory of ALL devices on the network (and their identity (such as certificate, unique IDs, etc.). An IoT Device Management platform can track devices, push configurations, and rotate credentials on a periodic basis. In some standards, proper identity management would mean long-term certificates are issued to each device at manufacturing, and then

that can be used to identify the device in any communication. Use widely accepted protocols such as **OAuth 2.0** or **ACE-OAuth** for IoT to facilitate authentication and authorization in a scalable manner.

User Awareness and Security Policies: While this is about devices, the users and administrators of those devices need to be brought into the loop. For IoT deployments, organizations should create clear security policies – that is, processes to approve new IoT devices, the network zones in which they're allowed, and what security features are required of vendors. Frequent training can also help avoid social engineering themes with IoT (i.e., do not install unofficial firmware). Consumer IoT security can benefit hugely from basic practices, such as changing default passwords during installation and segmenting the home Wi-Fi clump for use by IoT gadgets.

In practice, a defense-in-depth strategy, which includes a combination of the above mechanisms is encouraged. Just because a device has been taken over (maybe a zero-day exploit enabled it to bypass its authentication) doesn't mean that threat isn't detected and contained due to network monitoring and segmentation before serious damage is done. Meanwhile, promising new guidelines and frameworks (covered in Section 8) are starting to bundle best practices into concrete-to-do checklists for manufacturers and IoT operators.

To speak more, IoT security is not set once and done. Threats change,requiring a constant process of evaluation, patching and improvement. Next, we dive into real incidents to understand where defenses have failed and the lessons we can learn.

7 Case Studies

To define IoT Security issues that exist today, we show two real world examples of IoT Security incidents that have become symbolic of problems in the realm — The Mirai botnet attack and the Casino fish-tank thermometer breach. These cases demonstrate how IoT vulnerabilities get exploited and the effects of those attacks, as well as the security insights learned from them.

7.1 Mirai Botnet DDoS Attack (2016)

Regarded as a wake-up call for the perils of insecure IoT devices, the incident with the Mirai botnet has become a landmark case in IoT security. A malware **Mirai** infected IoT devices (such as IP cameras, digital video recorders (DVRs), and home routers) from August-October 2016 on the internet. Mirai worked by searching for devices open to the internet with Telnet or SSH ports that it could then try to log on to using a hardcoded list of 61 common default username/password combinations (admin/admin, root/12345, etc.). This straightforward strategy proved devastatingly successful – within weeks, Mirai had gained control of more than 600,000 IoT devices worldwide, cobbling them together into a botnet serving under the

command of the attackers.

Mirai enslaved devices that periodically connected back into a command-and-control server and could be directed to launch coordinated **Distributed Denial of Service (DDoS)** attacks. In late September 2016, Mirai dominated the news by carrying out some of the *largest DDoS attacks in history* up to that point. One of the targets was the site of cybersecurity journalist Brian Krebs, which was hit with traffic topping 600 Gbps, knocking his site offline. Shortly after, on October 21, 2016, Mirai was used to attack the DNS provider **Dyn** A deluge of over 1 Tbps (terabit per second) of bogus requests from tens of thousands of Mirai-infected devices overwhelmed Dyn's services. Since Dyn offered DNS for many popular sites (such as Twitter, Netflix, Reddit, etc.), the attack caused a huge disruption to the internet, in fact cutting off access to those sites for millions of users for hours. This was one of the earliest examples of IoT devices — such as CCTV cameras — indirectly making popular internet services unreachable in this way, on such a scale.

Analysis and Lessons: The Mirai case highlighted the shared risk, with a devastating impact, from IoT devices with inadequate security. Alone, a compromised webcam or DVR may seem inconsequential; but put these together by the hundred-thousand, and you have a digital army with the potential to take down vital internet guts. The key vulnerability that was exploited by Mirai was the widespread use of *default passwords* and lack of basic cyber hygiene for the IoT devices at users premises. The vast majority of devices that were infected by Mirai were still running factory default logins, or had telnet open with trivial passwords (some even harcoded). It highlights the importance of removing default credentials (a practice now prohibited by new emerging regulations in some countries), and encouraging users to alter device passwords at installation.

Mirai also demonstrated how quickly malware can spread when there's a lot of vulnerable systems out there, essentially acting as an internet-scale worm. It also underscored the difficulty in mitigation: unlike botnets of PCs, whose owners might complain of a slow computer or, say, install antivirus, IoT devices often languish unmanaged. Most of the owners of devices infected by Mirai didn't formulate their gadget as being part of an of a assault.

7.2 Casino Fish Tank Thermostat Breach (2017)

One notable example took place in 2017, when attackers found their way into a North American casino's network through an unlikely access point - a connected fish tank. The casino had set up a smart aquarium outfitted with networked sensors and a thermostat to automatically track the tank's environment. While this IoT device was a blessing for aquarium maintenance, it ended up being the weakest link in the casino's otherwise hardened network.

As the reports suggest (including one offered by the CEO of the cybersecurity firm Darktrace), the attackers identified a vulnerability in the fish tank's thermostat — it could have been an unpatched software flaw or default credentials —

that gave them remote access to the device. Once in the thermostat's control system, the attackers used that as a foothold to jump into the casino's wider network. They were able to move laterally through network segments, ultimately accessing a high-value database that included the personal information of the casino's VIP customers (the "high-roller" database). That sensitive data was then exfiltrated — in a sneaky move, attackers pulled the data back out using the fish tank thermostat itself, which would transmit the information, through the internet, to a remote server. Using the thermostat as the data conduit made it harder to detect as it may not have been monitored so closely as traditional endpoints.

The breach was eventually detected (Darktrace's anomaly detection AI allegedly flagged data being transferred out at an abnormal rate), but not before the data leaked. The attack and damage werenever publicly attributed, but the attack became widely cited as a cautionary tale in cybersecurity circles.

Analysis and Lessons: The casino aquarium hack is an example of a second type of attack, termed an **"IoT pivot"** – where a non-traditional network device is compromised to gain access to networks and assets behind security controls. The casino probably had robust security on the primary front lines (firewalls, intrusion detection for its server and so on), but the IoT thermostat was probably not protected or surveyed in a similar way. As Nicole Eagan of Darktrace pointed out, modern organizations have IoT devices from HVAC systems to personal assistants coming into their networks, and "it adds to the attack surface" that traditional defenses don't cover. This case underscores that security teams need to look past *every* connected device, even if it seems benign.

Technically, one of the lessons is network segregation and the principle of least privilege. Had the fish tank controller been air-gapped in a network segment with no route to the databases servers, the breach would have been confined to the device itself. The attackers were able to move from an IoT subnet to a database suggesting insufficient or misconfigured network segmentation. Enforcing strict internal network firewalls — allowing only the fish tank to communicate with its cloud service, for example — would restrict an intruder's lateral mobility.

The other lesson is that IoT devices must be hardened and monitored like any computer. That includes changing default credentials, applying patches and anomaly detection. Fortunately, anomaly detection did at least detect the anomalous data transfer (this is a success story for IoT security monitoring based on AI). Now many organizations use IT-specific security monitoring solutions that can monitor those anomalies, such as a smart thermostat suddenly broadcasting huge packets of data or connecting to an unknown external IP.

This story also brings the risk of data being stolen through IoT, Where Mirai focused on disruption, this was about espionage — demonstrating that IoT can be an attack vector for traditional data breaches. In industries such as hospitality, retail, or healthcare, attackers may also target IoT devices— including smart appliances, security cameras, or medical sensors—so that they can be used as easy ingress points to locate valuable data on the internal network.

8 Standards and Frameworks for IoT Security

Governments and industry groups worldwide responded by creating standards, best practice guidelines, and regulatory frameworks as IoT security concerns have increased. This is targeted at introducing defined recommendations (and in some cases, prescriptive approaches) to enhance the security baseline of IoT devices and associated deployments. Below we discuss some of the significant IoT security standards and frameworks:

- **OWASP IoT Top 10 (2018):** To raise awareness of common issues, the Open Web Application Security Project (OWASP) also provided a Top 10 list of IoT vulnerabilities. Some of the issues listed in the OWASP IoT Top 10 (2018) are *Weak, Guessable or Hardcoded Passwords*, *Insecure Network Services*, *Insufficient Privacy Protection*, *Lack of secure update mechanism*, *Lack of device management*, *Insecure Default Settings*, *Insecure data transfer and storage*, *Insecure or outdated components*, *Lack of physical hardening*,45089. This list has been applied extensively to raise awareness with IoT developers and acts as a checklist when developing or evaluating IoT systems. OWASP is not a regulatory body by any means, but its standards are well-known in the security world.

- **ETSI EN 303 645 (European IoT Security Standard):** In June 2020, the European Telecommunications Standards Institute (ETSI) released a standard for cybersecurity in consumer IoT, known as **EN 303 645**. This listing includes 13 standards that consumer IoT devices must follow, including the elimination of factory default passwords, the formulation of a vulnerability disclosure policy, the maintenance of software updates, the implementation of secure communication methods, limiting service exposure, and data privacy. Arguably, the most famous rule to come out of ETSI 303 645 is *Provision 5.1: No universal default passwords*-being, manufacturers must not use the same default password on all devices, which was in reaction to events such as Mirai. ETSI EN 303 645 has swiftly established itself as a de facto baseline reference on a global basis; UK and EU legislation (e.g. on the security of consumer IoT devices) drew heavily on ETSI EN 303 645. This standard, the note says "has become a reference for securing IoT devices across the globe, and is being employed by multiple cybersecurtiy regulations". For example, such products will require the user to set a unique password on first use, and provide a mechanism for secure software updates.

- **NIST IoT Cybersecurity Guidance:** In the United States, the National Institute of Standards and Technology (NIST) has published a series of reports on IoT cybersecurity. One of the foundational documents is **NISTIR 8259 (2020)**, "Foundational Cybersecurity Activities for IoT Device Manufacturers". This document provides recommendations to IoT device manufacturers on actions to take during design and development to ensure security

(for example, building in the capability for secure update, unique identification, logging, etc.). Additionally, NISTIR 8259A defines a core baseline of **IoT device cybersecurity capabilities** (like Device Identification, Device Configuration, Data Protection, Logical Access Control, Software Update, and Cybersecurity State Awareness). These baselines essentially enumerate what minimal security features an IoT device should have. Following NIST's guidance, the **IoT Cybersecurity Improvement Act of 2020** was enacted in the US, requiring that any IoT device purchased by the federal government meets the NIST-defined security criteria. This has ripple effects, since manufacturers who want to sell to the government must improve their practices. NIST has also issued guidance for IoT users (NISTIR 8228) on managing IoT risk at an organizational level.

- **ISO/IEC 27400:2022 (IoT Security and Privacy Guidelines):** At the international level, ISO and IEC have published standard 27400 in 2022 which gives high-level guidance on IoT security and privacy. It covers risk assessment specific to IoT and provides a taxonomy of security controls. Additionally, ISO has standards like **ISO/IEC 27030** (under development) focusing on IoT security techniques, and **ISO/IEC 30141:2018** which is an IoT reference architecture that includes a security framework. These ISO standards are often used by organizations seeking compliance or certification to demonstrate good security practices.

- **IoT Security Foundation Framework:** The IoT Security Foundation (IoTSF), an industry consortium, has released an *IoT Security Assurance Framework* (latest version 3.0 in 2021) which provides a comprehensive set of requirements and guidelines for IoT devices. It is mapped against other standards (like ETSI 303 645 and NIST) and covers areas from device hardware to cloud interface. Manufacturers and product developers can use it as a checklist to design secure products. The IoTSF also publishes best practice guides such as how to implement secure boot, manage vulnerability disclosures, etc.

- **Industrial and Sector-Specific Standards:** In the industrial IoT domain, the ISA/IEC 62443 series of standards (originally for industrial control systems security) are often applied. They provide a framework for security levels and processes in operational technology (OT) and IIoT environments. Similarly, the automotive industry's ISO 21434 (road vehicles cybersecurity engineering) becomes relevant as cars are essentially IoT nodes on wheels. Healthcare IoT devices might follow IEC 80001 (risk management for IT networks incorporating medical devices). While not IoT-specific, these vertical standards incorporate IoT scenarios.

- **Government Regulations and Baselines:** Various governments have introduced IoT cybersecurity regulations. For example, California's IoT Security Law (effective Jan 2020) requires that any IoT device sold in Cali-

fornia have "reasonable security features" – specifically calling out unique preprogrammed passwords or a requirement for user to set a password. The UK is moving forward with a law that mandates IoT manufacturers to follow certain guidelines (largely based on ETSI 303 645's top 3 requirements: no default passwords, vulnerability disclosure policy, and regular updates). These regulatory moves are pushing IoT security from a nice-to-have to a must-have in those markets.

- **Security Frameworks and Reference Architectures:** Organizations like the Industrial Internet Consortium (IIC) and NIST have proposed reference architectures that include security layers. NIST's *Cybersecurity Framework (CSF)* has also been adapted for IoT- providing a way to apply Identify/Protect /Detect/Respond/Recover functions to an IoT context. The **IoT Reference Architecture (IoT-RA)** by ISO (ISO 30141) includes a trustworthiness framework covering security, safety, reliability, resilience, and privacy.

9 Emerging Technologies and Approaches

Looking forward, several emerging technologies and novel approaches hold promise for strengthening IoT security. As the threat landscape evolves, so too must the defensive toolset. Here we discuss a few key developments:

Machine Learning and AI for IoT Security: Machine learning (ML), in particular, is increasingly applied to improve security monitoring and response in Internet of Things (IoT) networks. We briefly mentioned ML-based anomaly detection, which is able to model the normative behavior of IoT devices and report any deviations, potentially pointing at intrusions or malfunctions. As IoT devices create truly huge amounts of data, it's well within the wheelhouse of AI to work through logs and network traffic seeking patterns that would escape the notice of humans; for instance, advanced anomaly detection systems can tell not just if a single device is acting strangely but detect anomalies that cross from one device to another (maybe showcasing a slowly spreading worm before it reaches full bloom). ML models can also be used to help identify devices (i.e. fingerprint teh type of IoT devices based on their network behavior to know what is on the network), and this helps enforce security policy. One of the great challenges with AI in IoT security is being confident that models are good over time (retraining to avoid concept drift as usage patterns change) and explainable AI that make the decisions intelligible to a human analyst. However, early results are encouraging— one study claimed a significant improvement (14% increase in the detection rate at a lower false positive level) using ML for IoT anomaly detection. AI-driven security operations centers (SOCs) will also begin to incorporate IoT telemetry into their analysis, allowing for more proactive and adaptive defense.

Blockchain and Decentralized Security: Blockchain technology, known from cryptocurrencies, is being explored as a tool for IoT security. Features bordering on the essence of blockchain-decentralized trust, tamper-evident logs, and smart

contracts-can help overcome certain challenges in IoT. For example, this could be a blockchain where IoT devices write their identity and integrity data to a distributed ledger, making it difficult for an attacker to impersonate a device or introduce false data without detection. Since IoT transaction data (such as sensor readings or device configurations) recorded on blockchain cannot be altered without consensus, once written, blockchain's immutability should improve integrity and auditability of IoT data. One example is a Smart Contracts based access management on blockchain based system-it allows device access requests to happen through smart contracts that validate identities and usage policies. Other ideas are blockchain-based firmware update provenance: every firmware version could be hashed, with a digest written onto a ledger, allowing devices to compare any update against the blockchain to validate that it is a real release. One specific thing we can point to: a few are using blockchain to manage IoT device networks that don't have central authority-a network of smart appliances scattered across houses, say, could be using blockchain to share/threat intelligence or coordinate responses to anomalies without a central server. Blockchain can also assist with **device discovery and isolation**; if there is a compromised device then an entry in the blockchain can flag that identity, and smart contracts can automatically revoke its access to others (essentially consensus-driven quarantine). That said, blockchain in IoT is not a silver bullet: it can add complexity, and traditional blockchains (like Bitcoin) have high resource requirements which IoT devices cannot meet. To solve such issues, new lightweight, IoT-friendly consensus algorithms and permissioned blockchain models are developed. If these hurdles are crossed, blockchain can offer a robust framework for the security mechanisms of the IoT.

Edge and Fog Computing for Security: More IoT networks are bringing computation closer to devices and moving away from solely cloud architectures. The security can be achieved using **Edge computing** and **fog computing** paradigms; for example, rather than sending real-time data to the cloud for anomaly detection, an edge gateway can perform various analysis of data from local devices to determine whether there is a significant security risk and send the malicious traffic to the cloud instead which lowers the response time for both detection and programmatically securing the device in the case of attack. Edge devices can also work as security proxies for highly constrained sensors — performing encryption on their behalf, or aggregating and anonymizing data to prevent privacy loss. There are also forms of collaborative security emerging though: IoT devices at the edge working together to monitor their peer's behavior and vote on whether one of them may be compromised (a little like a localized consensus algorithm for trust). It resonates with decentralized ideas and can add to cloud-based oversight. **Zero Trust and Software-Defined Security:** Zero Trust Architecture (ZTA) is an evolving practice for IoT use cases. It includes micro-segmentation of networks so that communications for each IoT device are whitelisted and constantly authenticated. Dynamic and programmable flow control of networks is provided through technologies such as **Software-Defined Networking (SDN)** and **Network Function Virtualization (NFV)**. Orchestration of security that, for instance, auto-generates

an isolated micro-segment for each new IoT device, and pulls down a relevant firewall policy based on the device type in its construction, is a logical maturation step. One can expect the future of IoT security to be a combination of approaches that are more intelligent, self-governing, and distributed to tackle the threat landscape. AI will assist in handling complexity and faster response. Blockchain and distributed trust models may lessen dependency on central authorities and single points of failure. New cryptographic tools will take the initiative against threats that are beginning to emerge, such as quantum computing. Edge computing and software-defined controls will make the network and devices more adaptive. Although these emerging technologies aren't panaceas yet (and each has challenges to its own implementation), they are the continual innovation that must be employed to secure the increasingly proliferating IoT ecosystem.

10 Future Research Directions

While much progress has been made in identifying and addressing the threat to IoT devices and networks, there are still numerous areas with around–open challenges and room for further security, especially the areas are still ripe for exploratory data and systems. Below we list some directions for future research that may make an impact on IoT security in the next years:

- **Lightweight yet Strong Security Protocols:** Well, one line of research is the design of ultra-lightweight cryptographic protocols, purposefully designed for IoT use cases, and can provide strong security guarantees without overwhelming the limited resources of devices. Not just encryption algorithms (as we will see with PQC and lightweight crypto) but complete protocols for authentication, key management, and secure group communication.

- **AI Robustness and Collaborative Detection:** While machine learning has many advantages, adversarial machine learning is a risk area—the attackers may try to trick you into false positive anomaly detection or classification models (such as slightly changing their behavior to escape detection or poisoning the training set). Future work should lead to the development of HARML techniques targeting the future security of real-world IoTs.

- **Scalability and Self-Healing Networks:** The size and complexity of IoT networks will increase (5G/6G will enable massive machine-type communications). Scaling security architectures to millions of devices needs more research. One such idea is **self-healing IoT networks** – systems that can autonomously isolate and recover attacked nodes. This may include devices recognizing anomalous neighbor behavior from time to time and subsequently reconfiguring topology of the whole network on the fly to go around believed compromised nodes (applicable in particular case of mesh IoT networks)

- **Privacy-Enhancing Technologies:** As IoT frequently implies personal data, another direction is improvement of privacy preservation. There's also a need for research that looks into how users can be given more control and greater transparency about what data they share with their IoT devices and that they themselves collect. One way of doing this could be new privacy protocols (e.g. devices agreeing to share consent or enough data that it can only be repurposed low-value tasks like analysis, while also anonymizing any information before sending it to a central service in the cloud) or architectures that localize data processing as much as possible. One is edge computing for privacy: process sensitive information on-premises and only ship out aggregated and anonymized data.

- **Human Factors and Usable Security:** One of the aspects which is generally disregarded is the usability of IoT security. If ideally security measures are cumbersome, users may disable them or use devices insecurely. Research should focus on understanding human-IoT interaction and also propose interfaces that facilitate secure use of IoT devices. How do we communicate the security state of a smart home to a non-technical user, for example? Or how to make the process of securely onboarding a new device easier (e.g., NFC tap or QR codes for user-friendly, secure credential transfer)? Also some social aspects: how to incentivize manufacturers to care about security (consumer labeling schemes or mandatory insurance? would be a pure policy / economics project beyond technical research).

- **IoT-Specific Security Metrics and Benchmarks:** Metrics are required to track progress. Future work can work out what are the verifiable security properties we care about in IoT (not just traditional confidentiality/integrity/availability, but also safety, privacy, etc.) Creating standardized benchmarking criterion for security solutions on common IoT testbeds (with common workloads and attack scenarios) would aid in assessing relative effectiveness. This would be similar to something like the MLPerf benchmark for AI, but instead, for IoT security algorithms and devices.

To conclude, the IoT security landscape is ever-changing and multidisciplinary research – fusing discoveries in computer science (crypto, AI, formal methods) with knowledge from engineering (embedded systems, networking) and even social Sciences (user-behavior, economics of security) will serve to enhance IoT security. IoT devices will be smarter moving forward, not just in how they work, but in how they protect themselves, thanks to smarter software and support pillars surrounding them. Making sure that those advances materialize safely is the shared job of researchers and practitioners over the next 10 years.

11 Conclusion

The Internet of Things has had a significant impact on multiple industries, enabling greater automation, efficiency, and data utilization. Yet, this ubiquitous connectivity carries significant security risks as well. This essay describes the essential yet intricate realm of IoT safety, emphasizing the architecture of IoT These Type of systems and unique vulnerabilities that these systems expose and how they are exploited by attackers. We analyzed every layer of IoT ecosystem — sensors, network, and cloud — and identified common threats — weak passwords, open services, and device limitations. We also pointed out contemporary difficulties such as device diversity and insufficient built-in security. On the defensive front, we addressed BTCI solutions ranging from encryption, secure authentication, and network segmentation. The Mirai botnet and the casino breach are real-life examples where minor security weaknesses opened doors to wide-scale devastation. Next we explored how standards and frameworks coming from referenced organizations such as the NIST and OWASP working to create a bright future for IoT security.

Final Thought: IoT network security is a journey, not a destination. It requires a **multi-disciplinary initiative**: hardware design, software engineering, network architecture, policy making, and end-users all have a part to play. With a defense-in-depth strategy and a focus on staying ahead of new threat actors and developments, we can enjoy the rewards of more connected IoT capabilities without compromising security. The stakes are not just high — with IoT increasingly entangled in critical infrastructure and our everyday lives, securing IoT means securing our safety and our privacy. This term paper has attempted to comprehensively map the terrain of IoT security circa 2025, providing readers with both the conceptual frameworks and concrete examples needed to engage with this topic. The hope is that such knowledge will contribute to developing IoT systems that are not only smart and connected, but also secure and resilient by design.

References

[1] N. Eagan. There's a lot of iot... it expands the attack surface and most of this isn't covered by traditional defenses. *Business Insider via Hacker News*, 2018.

[2] OWASP Foundation. Owasp iot top 10 (2018). *OWASP Projects*, 2018.

[3] TechTarget. Top 12 iot security threats and risks to prioritize. *IoT Agenda*, 2023.