Evaluating Security and Data Privacy in Smart Home Devices

Natalia Khetagourova[†], Christoffer Lundh[†] and Joakim Kävrestad[*,†]

School of Engineering, Jönköping University, Sweden

Abstract

This research critically evaluated smart-home IoT-devices' data privacy and security practices Devices that self-declare CE compliance under EU RED directive 2014/53/EU were included. In response to escalating consumer risk due to unverified self-certification, a mixed-methods framework combining penetration testing, encryption analysis, and document analysis was applied to assess eight devices sold by European and Chinese retailers. The findings reveal a disparity in encryption standards, data transmission transparency, and compliance with EU expectations. European devices generally demonstrate stronger security configurations, while many Chinese devices expose users to significant privacy threats, including unauthenticated API use and third-party data routing. This study identifies systemic regulatory gaps in CE-mark enforcement and suggests mandatory third-party certification, increased transparency obligations, and regular legislative reassessments to bolster consumer protection in the evolving IoT ecosystem.

Keywords

Data Privacy, IoT Security, CE Self-Declaration, RED Directive, Smart Home, Regulatory Compliance, Penetration Testing

1. Introduction

This research examines how Internet of Things (IoT) devices manage user data and privacy, concentrating on variations based on a retailer's region of origin. It seeks to offer insights into IoT architecture, data privacy practices, and the effective use of connected technologies. In this research, we consider the security and privacy of IoT devices from a socio-technical perspective [1]. As been argued for in previous research [2, 3, 4], both cybersecurity and the IoT ecosystem are dependent on technology as well as the individuals and organizations where they are present. Further they are impacted by regulatory frameworks. Given the socio-technical perspective, the security and privacy on IoT devices are dependent in the interplay between those aspects [5]. In this research, we focus on the interplay between regulatory and technical aspects of security and privacy in IoT devices.

1.1. Problem statement

The global IT market is projected to reach 40 billion devices by 2030. Escalating cybersecurity risks accompany this growth; [6] reported a 400 % increase in IoT-targeted cyberattacks in 2023, noting that many smart home devices predominantly use insecure plain text communications (only 14.03 % used SSL/TLS) [7, 8]. In response to these threats, governmental agencies such as the European Union (EU) have enacted regulatory legislation to protect consumers. The CE-Marking (Conformité Européene) is mandatory for products marketed in the EU, and is used to indicate compliance with safety, health, and environmental standards. For IoT devices, CE-marking includes compliance with the Radio Equipment Directive (RED) 2014/53/EU, specifically Article 3(3)e, which mandates safeguards for user personal data and privacy protection [9, 10, 11]. Despite these regulations, the market is increasingly flooded with inexpensive Smart Home devices from Chinese online marketplaces [12]. The CE assessment is self-declaratory, relying on manufacturers' integrity [13]. Recent incidents, such as the FBI dismantling

The 11th International Workshop on Socio-Technical Perspectives in IS (STPIS'25) September 17-18 2025 Skopje, North Macedonia

*Corresponding author.

[†]Authors 1 and 2 contributed equally while author 3 had a supervising role.

joakim.kavrestad@ju.se (J. Kävrestad)

a botnet of 200,000 IoT devices linked to the People's Republic of China (PRC)[14], highlight the risks consumers face from potentially non-compliant devices, which contribute to cybersecurity threats regardless of their point of purchase. This experimental study compares IoT devices from official Swedish retailers against those from Chinese e-commerce retailers, evaluating their privacy and data security against EU Directive 2014/53/EU Article 3(3)e. This addresses whether consumers face similar data and privacy risks irrespective of the retailer's origin.

1.2. Research questions

Given the rapid increase in IoT devices and the reliance on self-declaration for CE marking, this study aims to determine what happens to consumers' data collected by smart home devices and examine whether the level of privacy and security differs based on the point of purchase.

Therefore, the research questions for this study were:

- **[1] How is the user's data and privacy managed and controlled in IoT devices?**
  This question addresses the issues of consumer trust and regulatory conformity by exploring how collected consumer data is stored and managed in the devices. Furthermore, insights gained from this analysis will provide evidence on whether manufacturers' standards align with stated EU expectations.
- **2] What differences can be identified between the tested IoT devices of European and Chinese products compared to the EU directive 2014/53/EU Article 3(3)e?**
  Considering that the smart home market is saturated with affordable IoT devices sold by Chinese e-commerce retailers, this question aims to identify the differences between the IoT devices tested in this study and EU Directive 2014/53/EU Article 3(3)e. The assessment will involve penetration testing the devices against the directive, clarifying whether the point of purchase affects the data and privacy security level in those devices.

1.3. Scope and limitations

This study focuses on identifying potential regional variations in CE compliance among retailers (point of purchase) rather than manufacturing standards, acknowledging that 32 % of all IoT devices are manufactured in China [15]. The study follows explicitly to EU Directive 2014/53/EU, Article 3(3)e, concerning radio equipment and data/privacy safeguards. Specific radio equipment categories (e.g., child monitors, wearables) were excluded due to supplemental regulations. This study does not perform a complete 2014/53/EU directive compliance assessment, excluding criteria beyond its scope (e.g., electrical, technical, safety standards). The methodology included penetration testing with simpler network monitoring tools for acquiring security and compliance data for analysis without advanced hardware manipulation. Furthermore, as the mobile phone used to enable the tests in this study was an Android, it regularly communicated with various Google servers and domains, since there were no appropriate ways to distinguish whether data sent to Google was related to IoT devices or the mobile phone, that data was excluded from the results.

2. Methodology

The research employed an experimental methodology which in three steps assessed devices included in this research. The experiment involved the following steps, and was repeated for each device:

1. **Setup** where we used a small network consisting of one computer, one mobile phone and the device we were testing, all connected to a simple wireless network with an internet connection. The general idea was to configure and manage the device using the cell phone, and to use the computer to conduct the experiments as outlined in steps 2-4.

Device name	Device type	Retailer
Ring Doorbell 5F97F2	Doorbell	EU
Deltaco SH-IPC16 Camera	Camera	EU
Cleverio CCT LB200 smart lightbulb	Lightbulb	EU
Cleverio Smart Mini Plug	Smartplug	EU
XW133-X9 Doorbell	Doorbell	China
v380 Pro Camera	Camera	China
Antela Smart Bulb E27	Lightbulb	China
Tuya Smart Socket F-ES01W	Smartplug	China

Table 1
Tested devices

2. **Vulnerability assessment** which involves identification of possible vulnerabilities that could be exploited [16]. This step involved both identification of vulnerabilities listed in public sources such as the CVE database [17], and using tools such at NMAP.
3. **Penetration testing** which involved attempts to use identified vulnerabilities to gain access to the tested devices, or data they sent over the network. The Penetration Test and Data Analysis Framework which is based on the IoT-PEN methodology for penetration testing of IoT devices was used [18, 19].
4. **Network analysis** where we analyzed network data to investigate where data traveled when being transferred between the mobile phone and the tested device.

Each experiment was conducted in an isolated laboratory network designed to mimic an average home network to ensure accurate and realistic data. Each device went through a BLE sniffing attack during setup while Wireshark was sniffing network traffic, followed by port scans and Man-In-The-Middle (MITM) attack methods to intercept the data. Once the penetration and vulnerability section of the experiment was completed and documented, the network analysis was initiated, focusing on security implementations, peer-to-peer, cloud, regional domains, and network protocols.

The collected data were then analyzed quantitatively and qualitatively, with a mixed methods analysis to summarize the average of the results. The quantitative analysis focused on encryption strength, data path transparency, and CE compliance rate, while the qualitative analysis focused on the devices' primary vulnerability and data-sharing concerns.

Since this thesis compares possible CE compliance differences in data privacy and security implementations between products sold by Chinese and European retailers, smart home devices in this study must be comparable in their technical specifications and functions to be suitable. Functional equivalence of the devices, such as video and voice communications, network connectivity, and associated mobile applications, ensured that observed variations in security implementation were not based on product category but on regional sales requirements. Eight devices in total were included in this research. They covered four different functions and for each function, one Chinese and one European device was included, as outlined in Table 1.

3. Results

This chapter presents the outcome of the experiments for each individual device, and the european devices are presented first. While most devices demonstrated positive compliance with EU Directive 2014/53/EU, Article 3(3)e, and implemented security measures, some exhibited minimal or no security features, transmitting data via cloud servers across various regions before reaching the mobile device. Our analysis focused on encryption, security implementations, API management, traffic routing, and involved domains. By monitoring network behavior and identifying domain involvement, we assessed the extent of third-party engagement, data management, and protection during device-to-device communication, such as video calls.

3.1. European devices

3.1.1. Ring Doorbell 5F97F2

Ring Doorbell (Amazon Inc.) was analyzed for security and network practices. This device costs approximately €100 and supports video, voice, and night vision. Network analysis revealed robust security protocol implementation, including TLSv1.2, HTTPS, DTLSv1.2, and transport protocols like TCP, UDP, QUIC, RTCP, RTP, and WebRTC for live streaming. Certificates were issued by Starfield Technologies Inc. for internal communication and DigiCert for external communication with Amazon cloud servers. The doorbell utilized RSA 2048 encryption and the TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 cipher suite, ensuring strong ephemeral session key generation. Both TLSv1.2 (device-to-cloud) and TLSv1.3 (app-to-cloud) were employed, indicating modern encryption.
Despite WebRTC enabling low latency, all device communications, including audio and video streaming, were consistently routed through Amazon cloud servers, even when the doorbell and mobile phone were on the same local network. STUN and TURN protocols and XOR-mapping for IP addresses facilitated this cloud-centric routing. Authentication involved cloud-based username verification and hashed fingerprints. STUN transactions were secured with HMAC-SHA1, and client usernames were Base64 encoded. Strong authentication was enforced during setup, including two-factor authentication, complex passwords, and email verification.
The doorbell and app exclusively communicated with Amazon and Ring-owned domains for device management, streaming, configuration, and analytics. No direct device-to-phone communication was observed. A significant privacy concern arose from the discovery of interactions with Facebook servers, suggesting potential data sharing by Amazon.

3.1.2. Deltaco SH-IPC16 Camera

The Deltaco SH-IPC16 Camera, manufactured by Deltaco (Sweden) and utilizing Tuya Inc.'s IoT cloud platform, was analyzed. Initial Nmap scans identified an open IRC port (6668) running IRC v7.95 alongside the Tuya IoT protocol. Despite the association of IRC with botnet activity, attempts to exploit vulnerabilities using Searchsploit, Exploitdb, HexChat, Netcat, and Metasploit, including Man-In-The-Middle and ARP spoofing, were unsuccessful in decrypting or intercepting traffic. Encrypted SSL handshakes prevented key retrieval, indicating initial resilience to basic exploitation. Network analysis via Wireshark revealed that when the phone and camera were on the same network, most TCP traffic, including video streams, was relayed through Amazon cloud servers. All application data and handshakes utilized TLSv1.2, with strong cipher suites (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 for Amazon and TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 for Tuya). However, a critical vulnerability was identified: Tuya's servers used self-signed certificates. This mandates the camera to accept them without validation, or rely on certificate pinning, creating a significant risk for MITM attacks, where an attacker could spoof a Tuya server to gain device access. When the phone and camera were on separate networks, communication was routed via a Telenor internet relay, with video streams sent as encrypted UDP. STUN packets were used for public IP determination and session keep-alives. All captured packets were securely encrypted, and no unauthorized data destinations were detected in this configuration. Minimal traffic was observed when the phone was idle or devices were on separate networks, even with push notifications.
A BLE sniffing session during device pairing was unsuccessful, suggesting the camera used a built-in access point (AP) for initial setup.

3.1.3. Cleverio CCT LB200 Lightbulb

The Cleverio CCT LB200 smart lightbulb (Kjell & Company, Sweden; approx. €20) was analyzed. It operates on the Tuya platform via the Smart Life app.
Reconnaissance confirmed the lightbulb as a Tuya device, with an IRC service detected on port 6668.

However, this was identified as a proprietary Tuya device-to-cloud communication protocol, not standard IRC. Despite attempts using Nmap, Searchsploit, msfdb, Wireshark, Bettercap, Telnet, Netcat, and Metasploit (including IRC-specific and Yeelight library exploits), no exploitable HTTP, HTTPS, SSL traffic, or vulnerabilities were found. Tuya's secure architecture and reliance on encrypted TLS (v1.2/1.3) communication effectively mitigated traditional MITM attacks, rendering tools like Burp Suite ineffective.
Network Analysis (Same Network): Most traffic was TCP between the mobile phone and Amazon cloud servers (Germany). Lightbulb-originated traffic included handshakes and TCP to US-based Amazon cloud servers and lifeaiot.com. All application data and handshakes were secured with TLSv1.2 and TLSv1.3, employing strong cipher suites like TLS_AES_123_GCM_SHA256 (for lifeaiot.com and Amazon) and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (for eu.lifeaiot.com). Certificates were legitimately issued by DigiCert. Despite strong encryption, data was observed leaving the local network to multiple Amazon and lifeaiot.com servers (Germany, US), even for local control.
Network Analysis (Separate Networks): Traffic to the phone primarily originated from Amazon cloud servers (TCP, TLSv1.2, TLSv1.3, and SSLv2), while outbound traffic from thephone mostly went to various eu.lifeaiot.com servers (TCP, TLSv1.3 for application data). Strong cipher suites (TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) and DigiCert-issued certificates were consistently observed for these communications.
A BLE sniffer captured a plaintext session/recognition token during the initial pairing process, though no further active BLE traffic was detected. This unencrypted token during pairing is a minor concern, but no further vulnerabilities were identified in BLE traffic or across iOS/Android platforms.

3.1.4. Cleverio Smart Mini Plug

The Cleverio Smart Mini Plug (Kjell & Company, Sweden; approx. €15), a Tuya device, was analyzed. Initial reconnaissance revealed that TCP port 6668 was open, characteristic of Tuya devices, but uniquely, it also exposed a Telnet-accessible service. Attempts to extract data via Telnet and Netcat were unsuccessful due to the custom Tuya protocol. However, fuzzing the Tuya protocol (starting with \x55\xAA) using Boofuzz successfully induced intermittent denial-of-service (DoS) attacks, temporarily freezing the plug.
Network Analysis (Same Network): DNS queries from the plug went to h3.iot-dns.com, while the phone communicated with third-party CDNs like cdn5th.com and cloudfront.net. The plug also connected to AWS EC2 instances in Germany and the UK. TLS handshakes utilized TLSv1.2 with the TLS_PSK_WITH_AES_256_CCM cipher suite, indicating a reliance on pre-shared key (PSK) authentication instead of more secure certificate-based methods.
Alarmingly, an over-the-air firmware update was intercepted. While encrypted, the firmware lacked digital signatures or certificate verification mechanisms. Analysis revealed clear-text code related to Zigbee communication, power management, and relay handling. Encrypted TCP traffic was recorded to and from China Unicom, a Chinese state-owned telecommunications operator, without a clear purpose or user consent.
Network Analysis (Separate Networks): Minimal encrypted cloud-bound traffic was observed. No peer-to-peer communication between the plug and the phone was detected, confirming all functionality is mediated by Tuya's cloud servers.
A plaintext identifier string, common to other Tuya products, was observed during BLE sniffing. While a stronger scanner might capture plaintext router credentials, the study's tools could not confirm this.

3.2. Chinese devices

3.2.1. XW133-X9 Doorbell

The XW133-X9 is a Chinese-manufactured smart home doorbell with video, voice, and night vision capabilities. It is cheap and popular, easily accessible by retailers like Amazon and Temu. With prices

Figure 1: Captured Video Feed from XW133-X9 MITM-Attack

ranging from €10 to €20, Temu was the point of purchase for this thesis.
During the network analysis, we found multiple vulnerabilities, such as unencrypted traffic, plaintext API, session keys, and video traffic. What made things interesting was the UDP video traffic, which was plain text, where we could identify the beginning of a JPEG File Interchange Format (JFIF) header and where the JFIF file ended. JFIF is a file format for pictures, and the fact that this was transmitted without any form of encryption meant that we could use a Python3 script to hijack and extract image data from the network communication between the doorbell and the mobile phone.
The script begins by identifying the JFIF header and locating the network interface and source port:

```
INTERFACE   = "Local Area Connection* 10"
SRC_PORT    = 10006
soi = buf.find(b'\xff\xd8\xff\xe0')
eoi = buf.find(b'\xff\xd9', soi)
```

The script then begins to listen and inspect each UDP packet from the selected network interface and source port, and extract everything between the beginning of the JFIF header and the end of the JFIF file in each packet. As it extracts frames from each packet, it will display and mirror the traffic on the attacker's computer, performing a live stream of the video footage in real-time, making this device extremely vulnerable to MITM attacks and Spyware. This is demonstrated by a caputured videoframe in Figure 1. The camera tracks movement in front of the device and sends an API call containing information about the activity, such as movement, alarms, and network information. This call is sent unencrypted with the API authentication token and could be extracted and manipulated similarly to video hijacking through MITM attacks.
The unencrypted traffic from the device was sent to cloud servers in the US region, especially towards the following domains: stark-industries.solutions, and naxclow.com, directly from the doorbell, even if the phone and doorbell were communicating on the same network. The application for receiving video calls and general communication between the doorbell and phone was more secure regarding encrypted traffic. However, it sent and received much traffic to and from China and the US. Even though the traffic was encrypted through HTTPS, QUIC, and TLSv1.3, it sent and received traffic, data, and API information from gac1.dcloud.net.cn. (CN), cm-10-178.getui.com. (CN), home.naxclow.com. (US), zjtelecom.com.cn (CN).
From the analyzed vulnerabilities and traffic behavior, the device was not compliant with EU Directive 2014/53/EU Article 3(3)e.

3.2.2. V380 Pro Camera

The v380 Pro Camera, a Chinese-made smart camera (€17 from Temu), offers motion detection, night vision, 360-degree rotation, and two-way voice.

Vulnerability assessment revealed critical security flaws despite some encrypted traffic (SSL, TLSv1.2 for handshakes, and UDP). API calls were sent in plaintext HTTP/1.0, using static identifiers, lacking authentication, session handling, and encryption. This exposed sensitive information like alarm types, developer IDs, hashed usernames, and passwords. Furthermore, commands like "DOWNGRD" and "UPGRD" were present, raising concerns about potential firmware manipulation if session keys were compromised. The static "macro-video IPC" User-Agent also enabled targeted attacks. While Nmap scans showed filtered/open ports limiting external communication, a BLE sniffer captured plaintext identification tokens ("BMV956 61237) during setup. SSL stripping attempts were mitigated by well-protected TLS handshakes, requiring server private key retrieval for decryption.

The camera's sole root certificate was issued by its manufacturer, GuangZhou HongShi CA Inc., raising security concerns due to the absence of neutral third-party certification.

Network analysis showed traffic routed from the camera to a China-based domain (95661237.nvdr.net) via a public Oracle cloud server before reaching the phone. Numerous UDP and TCP packets were sent directly to Alibaba Cloud Service in Singapore and China. While this data was encrypted (SSLv2, TLSv1.2), its contents were indecipherable, and no European cloud servers were involved.

Although the camera used encryption to protect personal data in transit, thereby partially fulfilling EU Directive 2014/53/EU Article 3(3)e, significant concerns remain due to plaintext API calls, the manufacturer acting as its certificate authority, and all traffic being routed through non-European manufacturer-controlled cloud servers before reaching the client's mobile phone.

3.2.3. Antela Smart Bulb

The Antela Smart Bulb E27 (€24 from Temu), a Wi-Fi-enabled light bulb operating via the Smart Life app, was analyzed.

Reconnaissance (Nmap, Searchsploit, Metasploit) indicated it is a Tuya-based product, similar to the Cleverio CCT LB200 light bulb, with an open IRC service on port 6668. This port uses a proprietary Tuya cloud communication protocol. Despite multiple attempts using various exploit tools (Netcat, Telnet, Metasploit, Yeelight Python3, Burp Suite, Hak5 Pineapple), no exploitable protocols effectively mitigated traditional MITM attacks. A BLE sniffer detected a plaintext session/identification token during initial pairing, but no further BLE activity was recorded post-setup.

Network Analysis (Same Network): DNS queries from the bulb went to h3.iot-dns.com. Open ports 443 and 8883 across Tuya Smart servers (Amazon-hosted in Germany, Ireland, and the US) were observed. TLSv1.2 handshakes were secured with robust cipher suites like TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (for a1-eu.lifeaiot.com via DigiCert) and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (for CloudFront via GoDaddy).

3.2.4. Tuya Smart Socket F-ES01W

The Tuya Smart Socket (Shenzhen, China; approx. €6-€7, from Temu) is an affordable wall plug with remote power and voice control (Alexa, Google Assistant).

Vulnerability assessment revealed an open port 6668 running the proprietary Tuya protocol v7.95 for secure device-to-cloud communication. Despite attempts to exploit common IRC vulnerabilities (e.g., UnrealIRCd) or perform banner leakage using Netcat and Telnet, no results were yielded. Similarly, attempts to force communication through a self-hosted IRC server (Hexchat) and SSL stripping attacks were unsuccessful, as all communication was encrypted with TLSv1.2.

Network Analysis (Same Network): DNS queries from the plug went to a3.tuyaeu.com and m2.tuyaeu.com, while the phone queried a1-eu.lifeaiot.com. Connections to these Tuya Smart servers (Amazon-hosted in Germany) used TCP with TLSv1.2. A recorded TLSv1.2 handshake with a1-eu.lifeaiot.com utilized TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 cipher suite and

a DigiCert-issued certificate. The mobile phone also transmitted encrypted UDP packets for device discovery, and peer-to-peer communication between phone and plug used TCP/TLSv1.2.

Network Analysis (Separate Networks): The plug maintained encrypted TLSv1.2 connections with Amazon-hosted Tuya cloud services. Another connection to an Amazon AWS Tuya Smart server on port 443 was noted. Though no certificates were recorded for this connection, the TLS handshake used the TLS_PSK_WITH_AES_128_CBC_SHA256 cipher suite, indicating use of PSK authentication.

BLE sniffing attempts were unsuccessful due to an apparent Bluetooth malfunction, with pairing relying solely on Wi-Fi.

Conclusion on security: Tuya Smart Socket demonstrated no exploitable vulnerabilities using standard assessment techniques. TLSv1.2 encryption and Tuya's proprietary protocol on port 6668 limited attack vectors. While the presumed Bluetooth malfunction and the use of PSK-based TLS (a minor concern, but still present) were noted, no plaintext data was discovered, and the plug appeared to be generally secure.

3.3. Data analysis

3.3.1. Quantitative analysis

The quantitative analysis focused on three main categories:

- **Encryption Strength** where the devices were scored based on how strong exnryption they use.
- **Data-Path Transparency** where devices were scored based on how they transkef data between the device and the mobile phone controlling it.
- *Compliance-Exploit Index* which is a metric that reflects if the device could be compromised in this text, and if it is compliant with the CE mark.

Each device was scored in every category on a scale from 1 to 4; the score was then summarized by calculating the average, median, and standard deviation. We then looked at regional differences using a Mann-Whitney U test on *Encryption Strength* and *Data-Path Transparency*. Finally, the *Compliance-Exploit Index* regional differences were visualized through bar charts.

The scores for each category were:

Encryption Strength:

1. No encryption, or legacy encryption.
2. TLSv1.0-1.1
3. TLSv1.2
4. TLSv1.3

Data-Path Transparency:

1. Cleartext
2. All traffic is routed via untrusted cloud servers.
3. Mixed peer-to-peer (P2P) and cloud via trusted European servers.
4. Direct P2P only.

Compliance-Exploit Index:

1. Compliant and Not Exploitable.
2. Compliant and Exploitable.
3. Non-Compliant and Not Exploitable.
4. Non-Compliant and Exploitable.

On average, European devices scored about one point higher than Chinese devices in encryption strength and transparency. As the calculations below show, EU devices used stronger ciphers and more direct data paths. However, there's quite a bit of overlap (especially in the Chinese scores), as shown by the standard deviations.

Encryption Strength

- **China**
  - Number of devices: 4
  - Mean = 2.25
  - Median = 2.5 (TLSv1.0-1.2)
  - Standard deviation ≈ 0.96
- **Europe**
  - Number of devices: 4
  - Mean = 3.25
  - Median = 3.0 (TLSv1.2)
  - Standard deviation = 0.50

Data-Path Transparency

- **China**
  - Number of devices: 4
  - Mean = 2.25
  - Median = 2.5
  - Standard deviation ≈ 0.96
- **Europe**
  - Number of devices: 4
  - Mean = 3.0
  - Median = 3.0
  - Standard deviation ≈ 0.82

Because our sample was small (n = 4 per region), we applied the Mann-Whitney U test to compare ranked scores without assuming a normal distribution, to see if European and Chinese devices differed on *Encryption Strength* and *Data-Path Transparency*. For *Encryption Strength*, the test statistic was U = 13.0 with P = 0.137; for *Data-Path Transparency*, U = 11.5 with p = 0.353. Both p-values exceed the 0.05 threshold, meaning we cannot rule out the possibility that the observed differences occurred by chance. In other words, although EU devices showed higher average scores, the evidence is insufficient to conclude a real regional gap.

As shown in Figure 2, 75% of European devices fall into Tier 1 (compliant and not exploitable) and the remaining 25% into Tier 2 (compliant but exploitable), while none appear in the high-risk Tier 4 (non-compliant and exploitable). In contrast, Chinese devices split evenly between Tier 1 (compliant and not exploitable) and Tier 4 (non-compliant and exploitable), with no devices in Tier 2 or 3. This shows that although half of the devices meet compliance, the other half fail the directive and remain exploitable, highlighting an apparent regional disparity in real-world security.

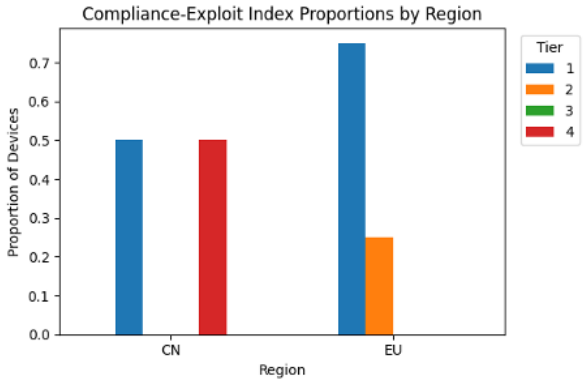

Figure 2: Compliance-Exploit Index Bar Chart

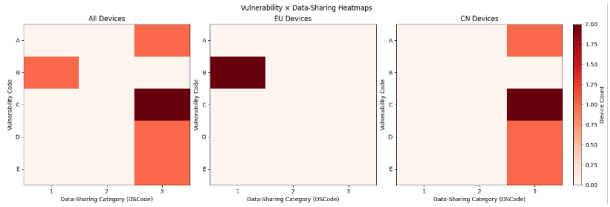

Figure 3: Vulnerability x Data-Sharing Heatmaps

3.3.2. Qualitative analysis

The qualitative analysis was divided into three heatmaps: all devices, European devices, and Chinese devices. Each heatmap presents a 5x3 matrix visualizing what security flaws exist and how those flaws coincide with data-sharing practices. Each device was coded by its primary vulnerability (A-E) and data-sharing category (1-3).

Primary vulnerability:

1. Plaintext traffic
2. Insecure certificates
3. Insecure API / Cleartext Authentication tokens
4. BLE Pairing weakness
5. MITM / Interception

Data-sharing category:

1. No third-party domains
2. Manufacturer cloud only
3. Multiple third-party domains

As seen in the heatmaps above, most of the vulnerabilities appeared in devices from the Chinese region. The most common vulnerability was insecure API calls or clear-text authentication tokens. The most common data-sharing concern was multiple third-party domains involved in communication between the device and the user's mobile phone.

3.3.3. Analysis summary

To combine our quantitative and qualitative findings, we present a joint display that aligns each region's average scores, compliance-exploit proportions, and dominant vulnerability x data-sharing pattern in a single table and heatmap.

Table summarizes for Europe and China:

Table 2
Summary of data analysis

Region	Avg. Encryption	Avg. Transparency	Tier 1	Tier 2	Tier 3	Tier 4	Top Combo
EU	3.3	3.0	75%	25%	0%	0%	B + DS 1
CN	2.3	2.3	50%	0%	0%	50%	C + DS 3

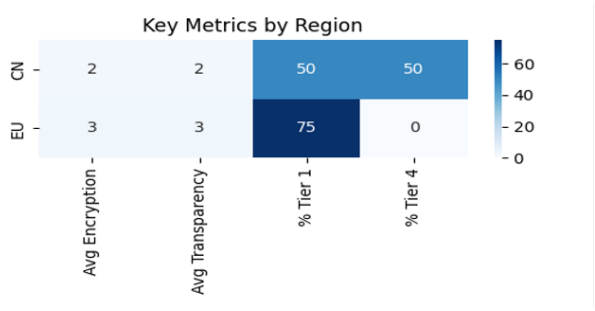

Figure 4: Summary heatmap

- Average *Encryption Strength* and *Data-Path Transparency* scores.
- Percentage of devices in each *Compliance-Exploit* tier (1-4).
- Most common vulnerability and data-sharing combination.

Table 2 and Figure 4 bring together our key findings. European devices average higher on Encryption Strength (3.3 vs. 2.3) and Data-Path Transparency (3.0 vs. 2.3), and 75% fall into the safest, compliant, and non-exploitable tier, with the remaining 25% in tier 2 as compliant and exploitable. Their most common issue is forced cloud-only routing without third-party sharing, which poses minimal risk. In contrast, Chinese devices split evenly between tier 1 (50%) and the most impactful tier, non-compliant and exploitable. Their top problem is unauthenticated API and cleartext token vulnerabilities, combined with multiple third-party routes, representing the worst technical weakness and privacy exposure alignment. This joint display shows that stronger encryption and tighter data paths in EU devices correspond to lower real-world risks. In contrast, weaker controls in Chinese devices coincide with higher exploitability and data-sharing concerns.

4. Discussion

This chapter provides an overview of the study's findings. It further discusses the study's implications and limitations and outlines its conclusions and recommendations.

4.1. Results discussion

Based on the results and discoveries, it is safe to say that a significant focus on security improvement has been implemented over the last few years, from IoT devices having no security at all to manufacturing companies such as Tuya improving security in most of their devices [20]. Some concerns still raise crucial questions, which will be further discussed in this chapter.

As the focus was on our research questions, which were:

1. How is the user's data and privacy managed and controlled in IoT devices?
2. What differences can be identified between the tested IoT-devices of European and Chinese products compared to the EU directive 2014/53/EU Article 3(3)e?

Many different encryption algorithms and innovative security solutions were found from device to device during the experiments. However, there have been a couple of outliers, such as a lack of security in device communication, weak encryption methods, mobile application security implementations, and questionable traffic routing.

4.1.1. Should the directive be changed?

The questionable traffic routing raises a fascinating and crucial question about the RED directive this study is based on: "*radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected*". As we have seen data from Chinese devices in this study being routed from IoT devices to the manufacturer's servers before it reaches the user's mobile phone, this opens privacy and security concerns. Still, as the traffic leaves the network encrypted, which would equal the safeguards, it meets the directive's requirements. A study conducted on 81 smart home devices in 2019 showed that 72 devices shared data with third parties such as Amazon, Akamai, and others that were completely unrelated to original manufacturer [21].

The directive's lack of update since 2014 and the rapid development of IoT devices and security threats indicate that it appears vague and outdated due to its wording. Considering how rapidly the IT world has been developing and expanding since 2014, ranging from smart home devices to AI and machine learning, Directive 2014/53/EU Article 3(3)e is a crucial directive in the European technological infrastructure.

With stricter regulations included in the directive, there would be less room for bypasses and loopholes, which would increase the security and privacy of European citizens, and with the hope that the European Union would regularly revisit any directives related to personal data and digital privacy, considering the rapidly expanding development of technology.

4.1.2. Contemporary Research and Commercial Practice

During the experiment phase of this study, it became evident that the security practices of some of the manufacturers have been updated and have become more secure. As discussed in previous chapters, IoT devices and, by extension, Smart Home devices are often designed to be compact and operate efficiently. Because of the structural nature of these devices, they usually have limited resources in processing power, memory, and battery life. While there are several emerging solutions, most of them come with a tradeoff, making the results from the experiments even more interesting because we can see solutions manufacturers have implemented to increase security in the devices within the structural limitations of the devices themselves.

By conducting experiments, we saw that most devices implement TLSv1.2 or 1.3 rather than SSL, a significantly higher number than reported in previous research. Some devices use DTLS1.2 for video and WebRTC+STUN/TURN to enhance security in real-time media transmission. This solution offers low-latency, end-to-end encryption with NAT traversal and per-session ephemeral keys that guard against eavesdropping and replay attacks.

Another example of good security practices observed was modern and robust cipher suites such as ECDHE (Elliptic Curve Diffie-Hellman Ephemeral), which leverages elliptic curve cryptography to establish secure key exchanges efficiently, ECDHE provides forward secrecy by generating ephemeral keys for each session, ensuring past session keys remain safe even if long-term keys are compromised [22].

During the network analysis phase, it was noted that almost all devices used certificates for server authentication, which is standard practice for securing TLS/DTLS sessions. However, not all certificates used independent validation (GoDaddy, DigiCert), making devices that utilize self-signed certificates vulnerable to spoofing.

In conclusion, while improved security in IoT devices is achievable, these enhancements often coexist with less secure practices. Although most tested devices comply with CE mark requirements, the protection and privacy of user data remain debatable [23]. This discussion sets the stage for the next section, which explores the relevance of the CE mark, or at least certain aspects of it.

4.1.3. Relevance of the CE-mark

Although the EU directive 2014/53/EU article 3(3)e aims to protect personal data and user privacy in IoT devices, this study's findings raise questions about its practical value. While devices may utilize robust

and modern encryption protocols during transmission, this alone does not ensure user privacy from downstream services where user data might be decrypted and processed. The integrity of the original encryption is compromised if user data is sold or shared with third parties and becomes decrypted, particularly if this occurs without proper oversight, leading to potential data leaks, as illustrated by earlier examples in this study. The 2014/53/EU directive aims for consumer protection; however, whether parts of the directive have shifted toward being more procedural than genuinely protective raises philosophical concerns, especially given that the CE mark is self-declaratory. Does the intended purpose of the 2014/53/EU Directive Article 3(3)e maintain its value in light of the security gaps in data transmission and the potential mishandling of user data thereafter?

While this study has identified weaknesses in the CE mark, some reforms could be applied to strengthen the CE mark in several ways. Based on the research conducted for this thesis, we have identified three critical points for improvement:

- End-to-end data protection: Ensuring not only data transmission but also secure storage, data processing, and data disposal. An enforced third-party validation practice for end-to-end protection would add consumer safety and trust.
- Transparency obligations: Manufacturers and service providers should be more transparent about how user data is handled regarding data sharing with third parties and make users aware that their data, including video recordings, might be decrypted and viewed.
- Frequent reassessment of the RED directive: The EU should reassess the RED directive in alignment with technological development to keep security in IoT devices up to date.

Without such or similar reforms, the CE mark may offer consumers little more than superficial assurance, exposing them to privacy risks, despite technical compliance.

4.2. Method discussion

Due to limitations in time and resources, the sample size of IoT devices had to be restricted. Arguably, a larger sample size could have yielded more variation in results, mainly since the majority of the IoT devices purchased for this study were unfortunately based on the same IoT architecture. However, during the device selection process, they were not identified as being produced by the same IoT developer; this connection was only discovered during the penetration testing.

The well-structured approach to data gathering also allowed for an iterative experimental process, enabling us to revisit and redo experiments as necessary while learning more about weaknesses and potential vulnerabilities in IoT devices. This provided an extensive and comprehensive dataset for the analysis phase of the study, answered the research questions, and generated thought-provoking insights into the world of cybersecurity for IoT devices, which were incorporated into the discussion and served as the basis for future research ideas.

5. Conclusions

Our findings demonstrate that, despite CE-marking, significant security and privacy vulnerabilities persist in IoT devices sold within and outside the EU. The rapidly increasing number of IoT devices, coupled with the current state of RED Directive 2014/53/EU Article 3(3)e, is insufficient to secure European citizens' data, as observed data often transits through multiple third-party domains globally. The self-declaration process for the CE mark poses a direct threat to personal data security, evidenced by plain text data transmission to manufacturers' servers. These observations reinforce claims by Cote et al. (2023) regarding unauthorized user data sales [24].

While our sample size was smaller than ThreatLabz's 2023 study [6] (which reported only 14.03% TLS usage), we observed a positive security progression: 75% of tested European devices used TLSv1.2, and 62.5% of Chinese devices used TLS1.0-1.2. Despite this improvement in encryption, the underlying issue of data being transmitted to third parties and the vulnerabilities of the self-declaration process

remain critical concerns. Studies show that users do not really understand what they are agreeing to and how their data is managed when accepting terms and policies[25].

5.1. Practical implications

This research highlights the unwitting privacy and security risks faced by European consumers using Wi-Fi-connected devices from both domestic and foreign retailers. The identified flaws in RED Directive 2014/53/EU Article 3(3)e and the lack of specific smart home device directives suggest an urgent need for strengthened regulations regarding product sales and privacy requirements for devices sold to European citizens. Our collected data can be used to raise awareness among policymakers and consumers regarding these critical privacy issues.

5.2. Scientific implications

Our experimental results significantly impact the scientific community, particularly in IoT development, system architecture, and user privacy implementation. The observed lack of privacy implementations and the limitations of the self-declaring CE mark indicate a clear research opportunity. This opens avenues for investigating new data authentication systems, such as a neutral third-party certification service, to control product data transmission routing before market release in Europe.

5.3. Future work

Future research could productively expand the device sample pool and geographical scope to include more countries, offering a broader global perspective on consumer exposure and standard adherence. Investigating user awareness and behavior regarding CE-marking and privacy risks would also be valuable in understanding consumer decision-making. Additionally, exploring how edge-based AI or federated learning could enhance local data privacy in smart devices offers promising insights. Lastly, researching the impact of user education and cybersecurity training on mitigating security gaps, without extensive legislative reform, warrants further studies such as [26].

Declaration on Generative AI

During the preparation of this work, the author(s) used Grammarly and ChatGPT in order to: Grammar and spelling check. The author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] S. H. Appelbaum, Socio-technical systems theory: an intervention strategy for organizational development, Management decision 35 (1997) 452–463.

[2] M. Malatji, S. Von Solms, A. Marnewick, Socio-technical systems cybersecurity framework, Information & Computer Security 27 (2019) 233–272.

[3] M. Malatji, A. Marnewick, S. von Solms, Validation of a socio-technical management process for optimising cybersecurity practices, Computers & Security 95 (2020) 101846.

[4] K. Ghaffari, M. Lagzian, M. Kazemi, G. Malekzadeh, A socio-technical analysis of internet of things development: an interplay of technologies, tasks, structures and actors, foresight 21 (2019) 640–653.

[5] J. M. Bauer, P. M. Herder, Designing socio-technical systems, in: Philosophy of technology and engineering sciences, Elsevier, 2009, pp. 601–630.

[6] Zscaler, 2023 enterprise iot ot threat report by zscaler threatlabz, https://www.zscaler.com/resources/2023-threatlabz-enterprise-iot-ot-threat-report, 2023. Accessed: 2025-06-11.

[7] M. W. Denko, A privacy vulnerability in smart home IoT devices, Ph.D. thesis, 2017.

[8] N. Singh, R. Buyya, H. Kim, Securing cloud-based internet of things: challenges and mitigations, Sensors 25 (2024) 79.
[9] E. Union, Radio equipment directive (red)., https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en, 2014. Accessed: 2025-06-11.
[10] E. Union, Ce-marking., https://single-market-economy.ec.europa.eu/single-market/ce-marking_en, 2021. Accessed: 2025-06-11.
[11] E. Union, Directive 2014/53/eu of the european parliament and of the council, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053, 2024. Accessed: 2025-06-11.
[12] NMSC, China smart home market, https://www.nextmsc.com/report/china-smart-home-market, 2024. Accessed: 2025-06-11.
[13] E. Commission, Ce-marking., https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm, 2024. Accessed: 2025-06-11.
[14] O. of Public Affairs., Court-authorized operation disrupts worldwide botnet used by people's republic of china state-sponsored hackers., https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state, 2024. Accessed: 2025-06-11.
[15] B. Kollmeyer, This chart shows the dramatic shift in global manufacturing over 30 years. the u.s. isn't at the top., https://www.marketwatch.com/story/this-chart-shows-the-dramatic-shift-in-global-manufacturing-over-30-years-the-u-s-isnt-at-the-top-37b6f62b, 2025. Accessed: 2025-06-11.
[16] S. Shah, B. Mehtre, A modern approach to cyber security analysis using vulnerability assessment and penetration testing, International Journal of electronics communication and computer engineering 4 (2013) 47–52.
[17] CVE, Cve™ program mission, https://www.cve.org/, ???? Accessed: 2025-06-11.
[18] G. Yadav, A. Allakany, V. Kumar, K. Paul, K. Okamura, Penetration testing framework for iot, in: 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), IEEE, 2019, pp. 477–482.
[19] G. Yadav, K. Paul, A. Allakany, K. Okamura, Iot-pen: A penetration testing framework for iot, in: 2020 International Conference on Information Networking (ICOIN), IEEE, 2020, pp. 196–201.
[20] F. Mehdipour, A review of iot security challenges and solutions, in: 2020 8th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC), IEEE, 2020, pp. 1–6.
[21] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, H. Haddadi, Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach, in: Proceedings of the Internet Measurement Conference, 2019, pp. 267–279.
[22] T. K. Goyal, V. Sahula, Lightweight security algorithm for low power iot devices, in: 2016 international conference on advances in computing, communications and informatics (ICACCI), IEEE, 2016, pp. 1725–1729.
[23] A. Orlowski, W. Loh, Data autonomy and privacy in the smart home: the case for a privacy smart home meta-assistant, AI & SOCIETY (2025) 1–14.
[24] M. Cote, W. Seymour, J. Pybus, D. Mariasin, A review on the risks and psychological harms presented by consumer iot products (2023).
[25] A. Hanlon, K. Jones, Ethical concerns about social media privacy policies: do users have the ability to comprehend their consent actions?, Journal of Strategic Marketing (2023) 1–18.
[26] J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos, S. Furnell, Evaluation of contextual and game-based training for phishing detection, Future Internet 14 (2022) 104.