広域スキャンシステムCensysを活用したIoTプラットフォーム探索の試行

彭 莎[1,a)]　インミンパパ[2,b)]　佐々木 貴之[2,c)]　吉岡 克成[1,2,d)]

概要：IoT プラットフォームは IoT デバイスやデバイスから収集されるデータを管理するための重要なバックエンドシステムであり，従来からサイバー攻撃の対象となっている．IoT プラットフォームのセキュリティ状態を調査するには，幅広い IoT プラットフォームを探索する必要がある．本研究では，広域スキャンシステム Censys を活用した IoT プラットフォームの探索を試行する．具体的には，IoT システムベンダ名と”IoT”, ”Smart”などのシンプルなキーワード，そして，ログインページを有するという条件を用いて Censys による検索を行い，検索結果の中からクラウドネットワーク上で動作するホスト群に着目することで IoT プラットフォームを発見する手法を検討する．

Exploration of IoT Platforms Utilizing Censys Internet-wide Scanning System

Sha Peng[1,a)]　Yinn Minn Pa Pa[2,b)]　Takayuki Sasaki[2,c)]　Katsunari Yoshioka[1,2,d)]

Abstract: As crucial backend systems for managing connected IoT devices and accumulated data, IoT platforms have become targets for cyberattacks. To investigate emerging security risks, it is necessary to explore a wide range of IoT platforms. This study aims to examine IoT platforms using the Internet-wide scanning system Censys. Specifically, we will conduct searches on Censys using simple keywords such as ”IoT” and ”Smart,” along with IoT system vendor names, and criteria including the presence of login pages. The focus will be on discovering IoT platforms by analyzing hosts operating on cloud networks within the search results.

1. Introduction

The rapid growth of the Internet of Things (IoT) has led to widespread deployment across various industries, homes, and public services, integrating countless devices into critical infrastructures. In these contexts, IoT platforms serve as centralized control and management layers, offering device onboarding, remote administration, data processing, inter-device communication, and cloud-based services. By functioning as the “nerve center” of the IoT ecosystem, these platforms play a crucial role in delivering scalable, intelligent solutions.

IoT platforms face significant security challenges due to their complex, modular architectures. Unlike end devices, they typically expose APIs and remote management interfaces, often integrating multiple third-party components that expand the attack surface. Consequently, breaches at the platform level can trigger large-scale service disruptions, data theft, or physical harm. For instance, in 2023, security flaws in Spireon systems allowed attackers to gain administrative access to millions of vehicles, enabling them to unlock doors and start engines [1]. Similarly, Toyota revealed that misconfigured cloud setups exposed sensitive customer data, such as vehicle locations and onboard device IDs [2]. Such examples underscore the profound risks posed

[1] Graduate School of Environment and Information Sciences, Yokohama, Kanagawa, 240–8501, Japan
[2] Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa, 240–8501, Japan
[a)] peng-sha-hf@ynu.jp
[b)] yinminn-papa-jp@ynu.ac.jp
[c)] sasaki-takayuki-yv@ynu.ac.jp
[d)] yoshioka@ynu.ac.jp

by compromised IoT platforms, which orchestrate billions of devices worldwide and provide remote management, data analysis, and mission-critical functions.

While much research has focused on the security of IoT end devices, IoT platform security, including attack surface analysis, vulnerability assessment, and targeted defense strategies, remains comparatively unexplored. To address this gap and provide insight into IoT platform exposure on the global Internet, this study leverages scanning results from the Internet-wide scanning engine Censys [3]. Specifically, we compile the names of 38 IoT platform vendors and simple IoT-related keywords, coupled with the "login-page" filter, to discover potential IoT platform hosts. We then employ a sampling-based process to validate each host, integrating manual inspection of its web management interface with Google-assisted cross-referencing of vendor documentation. Lastly, we examine the Autonomous System Number (ASN) to focus on cloud-based hosts and eliminate those belonging to Internet service providers, thus refining our focus to actual IoT platforms rather than end-user devices. By following these steps, we provide an initial outlook on the IoT platforms visible on the Internet.

By applying this approach, we found hosts associated with 8 of the 38 surveyed vendors that exhibit IoT platform characteristics. These outcomes not only validate the feasibility of systematic detection of IoT platforms via Censys using both keyword and filter-based strategies but also highlight that certain IoT platform hosts are directly exposed to the public Internet.

Overall, this study makes three principal contributions:

(1) `Systematic IoT Platform Identification`: We propose a scalable method that integrates Internet-wide scanning, keyword filtering, and ASN analysis to locate hosts potentially belonging to IoT platforms.

(2) `Empirical Evidence of IoT Platform Exposure`: Our findings show that some vendors' IoT platform hosts are publicly accessible, underscoring the security risks posed by such exposure in real-world scenarios.

(3) `Practical Insights for IoT Security Research`: By demonstrating how to discover IoT platform hosts within the vast pool of Internet-visible devices, this study provides a practical approach for future research on IoT ecosystem security and reducing the overall attack surface.

2. Related Work

The rapid expansion of the Internet of Things (IoT) has spurred significant research into the security, identification, and analysis of IoT systems. While much of the existing literature focuses on IoT devices, the security of IoT platforms — the infrastructure connecting and managing these devices — remains underexplored, particularly in the context of internet-wide discovery.

Several studies have investigated the security of specific IoT platforms. For instance, in 2023, B. Tejaswi et al. developed a security assessment framework to evaluate the core functions of 42 leading IoT management platforms. Their analysis revealed critical vulnerabilities, which enable unauthorized access, authentication failures, account takeovers, and remote code execution in some platforms [4].

Building on these findings, other researchers have explored methods to discover and analyze IoT platforms through Internet-wide scanning. In 2022, Said Jawad Saidi et al. proposed a method for identifying IoT backends by gathering backend IP addresses from various sources. Their study examined the operations of major IoT backend providers, utilizing domain data, DNS records, and traffic flow analysis to map the global distribution of IoT backends. Their findings revealed that some backends were concentrated in specific regions, posing risks related to regulatory compliance and cascading network failures [5].

Similarly, Ueda et al. presented two methods for discovering internet-facing On-Board Equipment (OBE) in connected vehicles. One method utilized web search to extract model information, while the other applied OBE-related keywords to Censys scan results. Their efforts identified over 2,500 exposed devices across 12 products [6].

3. Methodology

This section explains our approach for discovering and validating IoT platform hosts on the public Internet using the large-scale internet-scanning platform Censys.

Our methodology combines keyword-based querying, sampling-based validation, and ASN analysis to narrow down potentially exposed IoT platforms.

3.1 Search by Keywords

Censys is a specialized search engine for identifying and analyzing internet-connected systems. It continuously scans the public IPv4 space, infers application-

layer protocols, and uses DNS and redirects to detect active IPv6 addresses. By indexing these results, Censys provides an accurate, searchable view of the public Internet, allowing researchers to locate publicly accessible hosts, analyze service configurations, evaluate security risks, and track changes for cybersecurity and asset management. In this research, we employ Censys to identify IoT platforms that are exposed on the Internet.

IoT platforms typically require authentication to access, yet their login pages are often publicly accessible. If IoT-related keywords appear in an HTTP service, it suggests the host may belong to an IoT platform or a related management interface. Based on this principle, we defined the following search conditions in Censys:

- **Vendor Names:** We used 38 IoT platform vendors named in IoT Analytics "2023 IoT Software Companies" report [7], ensuring that hosts connected to these specific providers could be identified.
- **IoT-Related Keywords:** Alongside vendor names, we incorporated the generic terms "IoT," "Smart," and "Intelligent" because they commonly appear in official IoT documentation, enterprise solutions (e.g., "Smart Energy," "Intelligent Manufacturing"), and user forums, thus improving our coverage of potential IoT platforms.
- **"login-page" Filter:** We further refined our queries by employing the "login-page" label in Censys, which targets hosts that expose administrative or user-facing login interfaces—core features of IoT platforms.

For example, We used the following search pattern in Censys:

```
same_service(
http.response.body:"<VendorName>" and
http.response.body:"<IoTKeyword>" and
services.labels:"login-page" )
```

where <VendorName> and <IoTKeyword> are paired in every possible combination, yielding an initial set of hosts that may represent IoT platform deployments.

3.2 Sampling-Based Validation

3.2.1 Sampling and Verification Procedure

Given that some queries produced large result sets, we employed a sampling-based approach to verify candidates:

- **Host Sampling:** For each (VendorName, IoTKeyword) combination, we selected the top five Censys results for manual validation, optimizing efficiency under limited resources.
- **Manual Verification:** We inspected each host's web interface for signs of IoT platforms (e.g., vendor branding, product references, or relevant configuration details).
- **Google Cross-Referencing:** Any identifiable information (e.g., product name, technical terms) found on these interfaces was cross-checked using Google to locate supplementary evidence, such as official vendor documentation, that confirms a host's IoT platform status.
- **ASN Analysis:** For hosts that still appeared likely to be IoT platforms, we used IPinfo [8] to retrieve their Autonomous System Number (ASN) details. Those associated with residential ISPs were excluded, as they are likely end-user devices rather than actual IoT platforms. Conversely, ASNs belonging to corporations or cloud services indicate higher odds of true IoT platform infrastructure.

3.2.2 Criteria for Manual Identification

To ensure accurate identification of IoT platforms, the following criteria were defined (see Table 1):

- **Criteria 1: IoT Identity Verification**
  Confirming that the enterprise or product belongs to the IoT domain using publicly accessible information, such as official websites or product documentation.
- **Criteria 2: Host-Enterprise/Product Association**
  Verifying the presence of logos or names on the host to establish a connection with known IoT enterprises or products.
- **Criteria 3: IoT Functionality and Cloud Characteristics**
  Analyzing host-provided services and ASN classifications to verify alignment with IoT platform functionalities.

4. Results

In this chapter, we provide a detailed explanation of the experimental results obtained using the methodology proposed in Chapter 3, including both retrieval and validation outcomes.

4.1 Keywords Searching

Table 2 details the retrieval and sampling observations for each vendor-keyword combination. The "Vendor Name" column lists the 38 IoT platform vendors. The three subsequent columns present results for:

Table 1: Criteria for Manual Identification of IoT Platforms

Criteria ID	IoTPF Criteria	Criteria Details
Criteria 1	Confirms the authenticity of the IoT company or product.	The company focuses solely on IoT services or offers IoT solutions and services.
		Official documentation or introduction page available.
		The product description confirms IoTPF functionality.
		The product connects to IoT devices.
Criteria 2	Validates the host's link to the company or product.	The host's logo or name matches that of the company or product.
		The company's business scope aligns with the platform's features.
Criteria 3	Reflects IoT functionality and non-terminal device traits.	The host supports IoT protocols (e.g., MQTT, AMQP, CoAP), or official documentation confirms the use of IoT protocols and technologies.
		The host's ASN classification is not limited to being categorized as an ISP.

```
vendor + IoT + login-page
vendor + Smart + login-page
vendor + Intelligent + login-page
```

For each query, three metrics are recorded:

hit count: The total number of hosts returned by Censys for the given (vendor + keyword + login-page) search.

inspection count: The number of hosts actually sampled and manually examined.

IoTPF count: The number of hosts determined to be actual IoT platforms by manual inspection.

The final column, "Found IoT Platform," is set to "Yes" if at least a host is determined to be an IoT platform among the top five results for a particular vendor-keyword combination; otherwise, it remains "No".

Drawing on the data presented in Table 2 and focuses on two primary aspects: retrieval scale and keyword coverage. The details of these analyses are discussed below.

4.1.1 Significant Variations in Retrieval Scale

By examining Censys search results for each (vendor name + keyword + login-page) combination, we observed substantial differences in the number of returned hosts across both vendors and keywords:

- Major IT entities such as AWS, Microsoft, and Google can yield anywhere from a few thousand to hundreds of thousands of matched hosts when queried with "IoT," "Smart," or even "Intelligent." However, due to practical resource constraints, only the top five results were manually examined.
- In stark contrast, specialized vendors (e.g., Itac Software, TelkomIoT, OpenRemote) often showed zero or only a handful of matches under the same query conditions.

These findings suggest that while the (vendor name + keyword + login-page) approach is effective for identifying potential IoT platforms, differences in brand visibility and keyword usage lead to highly variable retrieval volumes for different vendors.

4.1.2 Keyword Coverage

Further analysis of the "IoT," "Smart," and "Intelligent" keywords reveals the following:

- Using "IoT" and "Smart" typically yields a greater number of results on Censys, particularly when searching for large-scale vendors.
- In contrast, searching for "Intelligent" produces fewer matches, with some cases returning no results at all. Nonetheless, its lower usage frequency can occasionally capture hosts overlooked by "IoT" or "Smart," thereby expanding the overall search coverage.

Based on these observations, "IoT" and "Smart" remain the most common and broadly effective keywords for locating public Internet IoT platforms. "Intelligent," though less prolific in raw match counts, can still prove useful for specific vendors or domain-focused branding.

This process identifies potential IoT platforms on the public Internet in line with our search strategy. However, keyword matches and login-page indicators alone cannot definitively confirm each hit as an actual IoT platform, necessitating further investigation through sampling-based validation and ASN analysis.

4.2 Verification

As summarized in Table 2, we searched for 38 IoT platform vendors on Censys using simple keyword combinations. We recorded the number of hits, the number of sampled checks, and the final count of determined IoT platforms. Table 3 provides further details on these determined platforms, including relevant key-

Table 2: Minimal Experimental Results

Vendor ID	Vendor Name	Search Result (Vendor Name + IoT + Login Page) (hit,inspection,IoTPF count)	Search Result (Vendor Name + Smart + Login) (hit, inspection, IoTPF count)	Search Result (Vendor Name + Intelligent + Login) (hit, inspection, IoTPF count)	Found IoT Platform
1	siemens	25,5,0	920,5,1	12,5,0	Yes
2	honeywell	6,5,0	78,5,0	8,5,0	No
3	bosch	76,5,0	1236,5,0	80,5,0	No
4	Schneider	13,5,1	38,5,1	9,5,0	Yes
5	AWS	1298,5,2	351,5,1	114,5,0	Yes
6	cisco	224,5,0	1450,5,0	48,5,0	No
7	microsoft	2624,5,3	23348,5,1	895,5,0	Yes
8	capgemini	3,3,0	2,2,0	1,1,0	No
9	dynatrace	3,3,0	0,0,0	3,3,0	No
10	ptc	7,5,0	11,5,0	3,3,0	No
11	google	1767,5,1	105074,5,0	1665,5,0	Yes
12	ABB	6,5,1	66,5,0	9,5,0	Yes
13	blynk	3,3,0	0,0,0	0,0,0	No
14	rockwell automation	16,5,0	13,5,0	4,4,0	No
15	andersen	0,0,0	4,4,0	0,0,0	No
16	itac software	0,0,0	0,0,0	0,0,0	No
17	topcon	0,0,0	3,3,0	1,1,0	No
18	telkomIoT	0,0,0	0,0,0	0,0,0	No
19	SAP	1041,5,1	1051,5,0	98,5,0	Yes
20	softwareAG	1,1,0	1,1,0	1,1,0	No
21	AVEVA	2,2,0	2,2,0	0,0,0	No
22	oracle	962,5,0	1374,5,0	30,5,0	No
23	advantech	9,5,0	4,4,0	2,2,0	No
24	tata consulancy services	0,0,0	0,0,0	0,0,0	No
25	IBM	2066,5,0	1333,5,0	98,5,0	No
26	beantech	0,0,0	1,1,0	0,0,0	No
27	wisepower	0,0,0	0,0,0	0,0,0	No
28	emerson	4,4,0	14,5,0	5,5,0	No
29	openremote	0,0,0	0,0,0	0,0,0	No
30	trimble	4,4,0	3,3,0	3,3,0	No
31	wellintech	0,0,0	0,0,0	0,0,0	No
32	hakunamatata	0,0,0	0,0,0	0,0,0	No
33	particle	39,5,3	119,5,0	15,5,0	Yes
34	salesforce	48,5,0	84,5,0	29,5,0	No
35	zebra	10,5,0	34,5,0	5,5,0	No
36	sciencesoft	0,0,0	0,0,0	0,0,0	No
37	infor	5,5,0	28,5,0	4,4,0	No
38	unifytwin	0,0,0	0,0,0	0,0,0	No

word(s) used for discovery, platform type or application domain, and the Autonomous System (AS) where each host resides. By examining these tables, we derive the following conclusions.

4.2.1 Verification Results

For each “vendor + keyword” combination, we manually inspected up to five hosts (or all if fewer than five were returned) based on the criteria and ASN analysis described in Section 3.2. Ultimately, eight vendors (e.g., Siemens, Schneider, AWS, Microsoft, Google, ABB, SAP, Particle) were found to have at least one determined IoT platform among their top five search results. This represents approximately 21% of the 38 vendors tested. In total, 16 hosts were determined to be providing IoT platform services.

Notably, a vendor name or branding found in a host’s HTML does not necessarily indicate direct operation by that vendor. Nonetheless, these hosts exhibited core IoT platform traits, suggesting that the vendor’s technology or branded products may have been incorpo-

Table 3: Overview of IoT Platform Hosts: Application Domains and Organizations

Vendor ID	Vendor Name	Keyword	Detected IoT Host	IoT Application Domain	AS Number & Organization
1	siemens	smart	Host 1	Industry IoT platform	AS16509 - Amazon.com, Inc.
4	Schneider	iot	Host 2	Smart building	AS14061 - DigitalOcean, LLC
		smart	Host 3	Smart building	AS8075 - Microsoft Corporation
5	AWS	iot	Host 4	Smart city	AS16509 - Amazon.com, Inc.
			Host 5	Smart city	AS16509 - Amazon.com, Inc.
		smart	Host 6	Industry IoT platform	AS16509 - Amazon.com, Inc.
6	Microsoft	iot	Host 7	Industry IoT platform	AS8075 - Microsoft Corporation
			Host 8	Track Monitoring	AS37963 - Hangzhou Alibaba Advertising Co.,Ltd.
			Host 9	Track Monitoring	AS37963 - Hangzhou Alibaba Advertising Co.,Ltd.
		smart	Host 10	Smart Park	AS31034 - Aruba S.p.A.
11	google	iot	Host 11	Smart meter	AS46606 - Unified Layer
12	ABB	iot	Host 12	Industry IoT platform	AS55990 - Huawei Cloud Service data center
19	SAP	iot	Host 13	Industry IoT platform	AS19318 - Interserver, Inc
33	particle	iot	Host 14	General IoT Platform	AS14061 - DigitalOcean, LLC
			Host 15	General IoT Platform	AS14061 - DigitalOcean, LLC
			Host 16	General IoT Platform	AS14061 - DigitalOcean, LLC

rated.

4.2.2 Effectiveness of Keyword Searches

Of the eight determined IoT platform vendors, seven were discovered using the 'IoT' keyword, underscoring the widespread usage of 'IoT' in documentation and service naming. Additionally, four vendors were identified through searches combining their names with "smart," revealing platforms that "IoT" did not capture. For instance, Siemens emerged only when paired with "smart," not "IoT." This finding suggests that not all IoT platforms explicitly label themselves as "IoT," and some may prefer "smart" or other domain-specific terminology. Consequently, although "IoT" provides the broadest coverage, supplementary keywords can uncover brand-oriented or scenario-specific platforms. Furthermore, no IoT platforms were detected using the "intelligent" keyword in our sampling.

4.2.3 Domain Diversity and Vertical Specialization

From the IoT Application Domain column in Table3, it is clear that determined IoT platforms span a variety of use cases. As outlined in Section 3.2, we validated each host's status as an IoT platform by examining available Web-UI information and cross-referencing identifiable terms (e.g., product names, technical keywords) through Google and official vendor documentation. In the process, we also established the IoT Application Domain for each platform, for example by consulting product brochures or manuals that clarified the platform's targeted use cases.

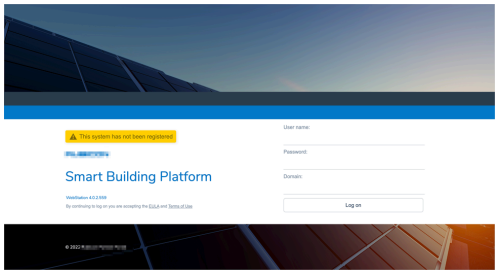

Figure 1: Host 3 Login Page

Some target multiple industries and general-purpose applications: for example, host 6 focuses on energy, water, and other industrial sectors, while host 14 integrates hardware modules, cloud management, and multiple communication pathways into a flexible, scalable solution. Meanwhile, other platforms serve more specialized verticals—for instance, host 3 is a third-party "smart building" solution based on Schneider's building management system. Figure 1 illustrates Host 3's login page, highlighting its role as a smart building platform. The official documentation further details its IoT architecture and features, confirming its application in the smart building sector. Overall, these findings show that IoT platforms exposed on the public Internet range from broad-based offerings to niche applications, demonstrating the IoT ecosystem's marked diversity and continuing evolution.

In summary, the "vendor + keyword + login-page" approach effectively identifies IoT platforms on the pub-

lic Internet, although retrieval volumes vary considerably. Large-scale vendors often yield numerous results, whereas specialized vendors may produce few or none. While “IoT” and “Smart” generally achieve broader coverage, “Intelligent” can, in certain cases, capture platforms overlooked by the other two. Verification shows that among 38 vendors tested, 8 (approximately 21%) had at least one determined IoT platform in the top five search results, totaling 16 verified hosts. Among these 8 vendors, 7 could be discovered using the ‘IoT’ keyword, and 4 could also be found using ‘Smart’, underscoring the importance of keyword choice; no additional IoT platforms were uncovered with “Intelligent.” Overall, these findings confirm the feasibility of our search methodology and, through an examination of platform application scenarios, highlight the diverse and rapidly evolving nature of IoT platforms exposed on the public Internet.

5. Discussion

This study systematically explored IoT platform hosts potentially exposed on the public Internet by combining vendor names, general IoT-related keywords (e.g., “IoT,” “Smart,” “Intelligent”), and Censys's “login-page” filter. Our findings yield four primary insights:

5.1 Importance of Multi-Keyword Strategies

Approximately 21% of the surveyed vendors had hosts exhibiting IoT platform traits among the top five Censys results, suggesting the viability of pairing basic IoT keywords with login-page queries. Notably, “Smart” occasionally identified IoT platforms missed by the keyword “IoT,” indicating that many platforms do not explicitly label themselves as such. Some deploy “Smart” or domain-specific terminology instead. Hence, broadening keyword usage is advisable to capture the full range of exposed IoT platforms.

5.2 Extended Searching with Specific Signatures

Among the 16 IoT platforms analyzed in this study, examining each host's unique signatures and expanding the search in Censys could potentially uncover additional hosts running the same platform. To illustrate, we focus on Host 3, a smart building IoT platform, detailing specific search strategies and results. In this trial, we utilized a specific string from the HTML title of Host 3 as a signature:

```
services.http.response.html_title:
"[Anonymized]"
AND
autonomous_system.description:
{"Amazon","DigitalOcean","Microsoft
Corporation","Alibaba","Aruba",
"Unified Layer","Huawei Cloud",
"Interserver"}
```

We identified 35 matches and manually reviewed all of them. Among these, 29 were identified as operational Schneider IoT platforms, with three hosts exposing their UI for demonstration purposes, and two others associated with a different IoT platform offering smart building services. Four hosts were inaccessible. This highlights the potential for expanding searches using customized signatures of identified platforms.

5.3 Limitations of Detection Scope

While our approach broadens the scope of IoT platform detection compared with earlier studies, several limitations persist. Rather than targeting only a handful of well-known IoT vendors, we included 38 providers from industry reports, capturing a more diverse range of organizational backgrounds. In addition, our use of generic keywords (“IoT,” “smart,” “intelligent”) is not confined to any specific application domain, enabling detection across multiple industries.

However, because our method relies heavily on web-facing login pages, platforms offering only API endpoints—without a standard user interface—are likely to be overlooked. To address this gap, future work could scan widely used IoT protocols (e.g., MQTT, AMQP) or employ machine-learning techniques to infer IoT-specific traits from network traffic, thereby capturing platforms without a traditional login page.

5.4 Verification Constraints

Verification relied on sampling the top five results per query and cross-referencing with Google to confirm the authenticity of IoT platforms. While efficient under limited resources, this procedure may miss lower-ranked or differently labeled platforms. In addition, using ASN analysis to exclude broadband ISP networks helps eliminate consumer endpoints but may also omit relevant hosts (e.g., private enterprise or partner networks) in edge cases.

In summary, our study affirms that combining vendor names, IoT-related keywords, and login-page filtering in

Censys can effectively detect IoT platforms on the public Internet, a finding further evidenced by the direct accessibility of certain platform hosts. The risks vary across vendors and deployment styles, indicating that security measures must extend beyond end devices. As the "data and logic hub" of IoT infrastructures, the IoT platform itself constitutes a substantial attack surface that merits greater attention from both industry and researchers.

6. Conclusion and Future Work

This study employed the Internet-wide scanning engine Censys to identify and analyze hosts associated with 38 Internet of Things (IoT) vendors. We performed keyword-based searches ("IoT," "Smart," "Intelligent") in conjunction with a "login-page" filter, followed by sampling verification and Autonomous System Number (ASN) analysis. Experiments show that this method reliably detects IoT platforms on the public Internet: of the 38 vendor queries, around 21% (eight vendors) had IoT platforms among the top five Censys results, totaling 16 determined IoT platform hosts. Specifically, seven vendors emerged when paired with the "IoT" keyword and four when paired with "Smart," whereas "Intelligent" produced no additional findings. Notably, these 16 verified IoT platforms span a broad range of industries and verticals, highlighting both the ecosystem's diversity and its associated security risks.

From a practical standpoint, this work offers several crucial insights. First, correlating host information with ASN data can more accurately illuminate how IoT platforms are exposed on the Internet. Second, confirming external connectivity to IoT vendor hosts in public networks enables stakeholders to better evaluate attack surfaces and potential threats. Finally, the keyword- and "login-page"-based search approach presented here provides a feasible automated method for platform identification in large-scale and heterogeneous IoT environments. Future research can be expanded as follows:

(1) `Expansion of the keyword set`
Incorporate multiple languages and domain-specific IoT terms to encompass a broader array of vendors and application scenarios, thus enhancing both coverage and accuracy.

(2) `Enhanced filtering criteria`
Supplement Censys queries with additional IoT-specific indicators to discover more exposed hosts without sacrificing precision. Systematically combining richer filter parameters may reveal previously undiscovered or hidden IoT platforms.

(3) `Automated identification`
Future work could explore automated approaches or NLP techniques for analyzing login pages, product names, and API information. These methods could validate IoT hosts more efficiently at scale and reduce manual verification overhead.

(4) `Security assessment`
Correlating the identified IoT hosts with vulnerability databases (e.g., CVE), or honeypot data could enable a more comprehensive, quantitative analysis of actual risks and attack surfaces.

(5) `Cross-validation with other platforms`
Utilizing additional internet-wide scanning services such as Shodan or ZoomEye for cross-referencing could further broaden overall coverage and clarify the scope of IoT platform exposure.

謝辞 A part of this paper is based on results obtained from a project, JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

参考文献

[1] Sam Curry and Neiko Rivera and Brett Buerhaus and Maik Robert and Ian Carroll and Justin Rhinehart and Shubham Shah ：Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More(online), 入手先 ⟨https://samcurry.net/web-hackers-vs-the-auto-industry#credits⟩ (2023.01.03).

[2] response：Toyota announces new vehicle information leaks: 260,000 Lexus owners(online), 入手先 ⟨https://response.jp/article/2023/06/01/371625.html⟩ (2023.06.01).

[3] Durumeric, Z., Adrian, D., Mirian, A., Bailey, M. and Halderman, J. A.: A Search Engine Backed by Internet-Wide Scanning, 22nd ACM Conference on Computer and Communications Security, (2015).

[4] Tejaswi, B., Mannan, M. and Youssef, A.: All Your IoT Devices Are Belong to Us: Security Weaknesses in IoT Management Platforms, Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy, pp. 245–250, 2023.

[5] Saidi, S. J., Matic, S., Gasser, O., Smaragdakis, G. and Feldmann, A.: Deep dive into the IoT backend ecosystem, Proceedings of the 22nd ACM Internet Measurement Conference, pp. 488–503, 2022.

[6] Ueda, T., Sasaki, T., Yoshioka, K. and Matsumoto, T.: An Internet-Wide View of Connected Cars: Discovery of Exposed Automotive Devices, Proceedings of the 17th International Conference on Availability, Reliability and Security, Article No. 146, 2022.

[7] Dimitris Paraskevopoulos：The leading IoT software companies 2023 (online), 入手先 ⟨https://iot-analytics.com/leading-iot-software-companies/⟩ (2023.04.12).

[8] IPinfo.io：IP Address Geolocation and Threat Intelligence (online), 入手先 ⟨https://ipinfo.io/⟩ (2024.01.12).