Abbas Moallem (Ed.)

LNCS 14045

HCI for Cybersecurity, Privacy and Trust

5th International Conference, HCI-CPT 2023
Held as Part of the 25th HCI International Conference, HCII 2023
Copenhagen, Denmark, July 23–28, 2023
Proceedings

Springer

Lecture Notes in Computer Science **14045**

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.

LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.

Abbas Moallem
Editor

HCI for Cybersecurity, Privacy and Trust

5th International Conference, HCI-CPT 2023
Held as Part of the 25th HCI International Conference, HCII 2023
Copenhagen, Denmark, July 23–28, 2023
Proceedings

Springer

Editor
Abbas Moallem
San Jose State University
San Jose, CA, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-35821-0 ISBN 978-3-031-35822-7 (eBook)
https://doi.org/10.1007/978-3-031-35822-7

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

Human-computer interaction (HCI) is acquiring an ever-increasing scientific and industrial importance, as well as having more impact on people's everyday lives, as an ever-growing number of human activities are progressively moving from the physical to the digital world. This process, which has been ongoing for some time now, was further accelerated during the acute period of the COVID-19 pandemic. The HCI International (HCII) conference series, held annually, aims to respond to the compelling need to advance the exchange of knowledge and research and development efforts on the human aspects of design and use of computing systems.

The 25th International Conference on Human-Computer Interaction, HCI International 2023 (HCII 2023), was held in the emerging post-pandemic era as a 'hybrid' event at the AC Bella Sky Hotel and Bella Center, Copenhagen, Denmark, during July 23–28, 2023. It incorporated the 21 thematic areas and affiliated conferences listed below.

A total of 7472 individuals from academia, research institutes, industry, and government agencies from 85 countries submitted contributions, and 1578 papers and 396 posters were included in the volumes of the proceedings that were published just before the start of the conference, these are listed below. The contributions thoroughly cover the entire field of human-computer interaction, addressing major advances in knowledge and effective use of computers in a variety of application areas. These papers provide academics, researchers, engineers, scientists, practitioners and students with state-of-the-art information on the most recent advances in HCI.

The HCI International (HCII) conference also offers the option of presenting 'Late Breaking Work', and this applies both for papers and posters, with corresponding volumes of proceedings that will be published after the conference. Full papers will be included in the 'HCII 2023 - Late Breaking Work - Papers' volumes of the proceedings to be published in the Springer LNCS series, while 'Poster Extended Abstracts' will be included as short research papers in the 'HCII 2023 - Late Breaking Work - Posters' volumes to be published in the Springer CCIS series.

I would like to thank the Program Board Chairs and the members of the Program Boards of all thematic areas and affiliated conferences for their contribution towards the high scientific quality and overall success of the HCI International 2023 conference. Their manifold support in terms of paper reviewing (single-blind review process, with a minimum of two reviews per submission), session organization and their willingness to act as goodwill ambassadors for the conference is most highly appreciated.

This conference would not have been possible without the continuous and unwavering support and advice of Gavriel Salvendy, founder, General Chair Emeritus, and Scientific Advisor. For his outstanding efforts, I would like to express my sincere appreciation to Abbas Moallem, Communications Chair and Editor of HCI International News.

July 2023 Constantine Stephanidis

HCI International 2023 Thematic Areas and Affiliated Conferences

Thematic Areas

- HCI: Human-Computer Interaction
- HIMI: Human Interface and the Management of Information

Affiliated Conferences

- EPCE: 20th International Conference on Engineering Psychology and Cognitive Ergonomics
- AC: 17th International Conference on Augmented Cognition
- UAHCI: 17th International Conference on Universal Access in Human-Computer Interaction
- CCD: 15th International Conference on Cross-Cultural Design
- SCSM: 15th International Conference on Social Computing and Social Media
- VAMR: 15th International Conference on Virtual, Augmented and Mixed Reality
- DHM: 14th International Conference on Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management
- DUXU: 12th International Conference on Design, User Experience and Usability
- C&C: 11th International Conference on Culture and Computing
- DAPI: 11th International Conference on Distributed, Ambient and Pervasive Interactions
- HCIBGO: 10th International Conference on HCI in Business, Government and Organizations
- LCT: 10th International Conference on Learning and Collaboration Technologies
- ITAP: 9th International Conference on Human Aspects of IT for the Aged Population
- AIS: 5th International Conference on Adaptive Instructional Systems
- HCI-CPT: 5th International Conference on HCI for Cybersecurity, Privacy and Trust
- HCI-Games: 5th International Conference on HCI in Games
- MobiTAS: 5th International Conference on HCI in Mobility, Transport and Automotive Systems
- AI-HCI: 4th International Conference on Artificial Intelligence in HCI
- MOBILE: 4th International Conference on Design, Operation and Evaluation of Mobile Communications

List of Conference Proceedings Volumes Appearing Before the Conference

1. LNCS 14011, Human-Computer Interaction: Part I, edited by Masaaki Kurosu and Ayako Hashizume
2. LNCS 14012, Human-Computer Interaction: Part II, edited by Masaaki Kurosu and Ayako Hashizume
3. LNCS 14013, Human-Computer Interaction: Part III, edited by Masaaki Kurosu and Ayako Hashizume
4. LNCS 14014, Human-Computer Interaction: Part IV, edited by Masaaki Kurosu and Ayako Hashizume
5. LNCS 14015, Human Interface and the Management of Information: Part I, edited by Hirohiko Mori and Yumi Asahi
6. LNCS 14016, Human Interface and the Management of Information: Part II, edited by Hirohiko Mori and Yumi Asahi
7. LNAI 14017, Engineering Psychology and Cognitive Ergonomics: Part I, edited by Don Harris and Wen-Chin Li
8. LNAI 14018, Engineering Psychology and Cognitive Ergonomics: Part II, edited by Don Harris and Wen-Chin Li
9. LNAI 14019, Augmented Cognition, edited by Dylan D. Schmorrow and Cali M. Fidopiastis
10. LNCS 14020, Universal Access in Human-Computer Interaction: Part I, edited by Margherita Antona and Constantine Stephanidis
11. LNCS 14021, Universal Access in Human-Computer Interaction: Part II, edited by Margherita Antona and Constantine Stephanidis
12. LNCS 14022, Cross-Cultural Design: Part I, edited by Pei-Luen Patrick Rau
13. LNCS 14023, Cross-Cultural Design: Part II, edited by Pei-Luen Patrick Rau
14. LNCS 14024, Cross-Cultural Design: Part III, edited by Pei-Luen Patrick Rau
15. LNCS 14025, Social Computing and Social Media: Part I, edited by Adela Coman and Simona Vasilache
16. LNCS 14026, Social Computing and Social Media: Part II, edited by Adela Coman and Simona Vasilache
17. LNCS 14027, Virtual, Augmented and Mixed Reality, edited by Jessie Y. C. Chen and Gino Fragomeni
18. LNCS 14028, Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management: Part I, edited by Vincent G. Duffy
19. LNCS 14029, Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management: Part II, edited by Vincent G. Duffy
20. LNCS 14030, Design, User Experience, and Usability: Part I, edited by Aaron Marcus, Elizabeth Rosenzweig and Marcelo Soares
21. LNCS 14031, Design, User Experience, and Usability: Part II, edited by Aaron Marcus, Elizabeth Rosenzweig and Marcelo Soares

22. LNCS 14032, Design, User Experience, and Usability: Part III, edited by Aaron Marcus, Elizabeth Rosenzweig and Marcelo Soares
23. LNCS 14033, Design, User Experience, and Usability: Part IV, edited by Aaron Marcus, Elizabeth Rosenzweig and Marcelo Soares
24. LNCS 14034, Design, User Experience, and Usability: Part V, edited by Aaron Marcus, Elizabeth Rosenzweig and Marcelo Soares
25. LNCS 14035, Culture and Computing, edited by Matthias Rauterberg
26. LNCS 14036, Distributed, Ambient and Pervasive Interactions: Part I, edited by Norbert Streitz and Shin'ichi Konomi
27. LNCS 14037, Distributed, Ambient and Pervasive Interactions: Part II, edited by Norbert Streitz and Shin'ichi Konomi
28. LNCS 14038, HCI in Business, Government and Organizations: Part I, edited by Fiona Fui-Hoon Nah and Keng Siau
29. LNCS 14039, HCI in Business, Government and Organizations: Part II, edited by Fiona Fui-Hoon Nah and Keng Siau
30. LNCS 14040, Learning and Collaboration Technologies: Part I, edited by Panayiotis Zaphiris and Andri Ioannou
31. LNCS 14041, Learning and Collaboration Technologies: Part II, edited by Panayiotis Zaphiris and Andri Ioannou
32. LNCS 14042, Human Aspects of IT for the Aged Population: Part I, edited by Qin Gao and Jia Zhou
33. LNCS 14043, Human Aspects of IT for the Aged Population: Part II, edited by Qin Gao and Jia Zhou
34. LNCS 14044, Adaptive Instructional Systems, edited by Robert A. Sottilare and Jessica Schwarz
35. LNCS 14045, HCI for Cybersecurity, Privacy and Trust, edited by Abbas Moallem
36. LNCS 14046, HCI in Games: Part I, edited by Xiaowen Fang
37. LNCS 14047, HCI in Games: Part II, edited by Xiaowen Fang
38. LNCS 14048, HCI in Mobility, Transport and Automotive Systems: Part I, edited by Heidi Krömker
39. LNCS 14049, HCI in Mobility, Transport and Automotive Systems: Part II, edited by Heidi Krömker
40. LNAI 14050, Artificial Intelligence in HCI: Part I, edited by Helmut Degen and Stavroula Ntoa
41. LNAI 14051, Artificial Intelligence in HCI: Part II, edited by Helmut Degen and Stavroula Ntoa
42. LNCS 14052, Design, Operation and Evaluation of Mobile Communications, edited by Gavriel Salvendy and June Wei
43. CCIS 1832, HCI International 2023 Posters - Part I, edited by Constantine Stephanidis, Margherita Antona, Stavroula Ntoa and Gavriel Salvendy
44. CCIS 1833, HCI International 2023 Posters - Part II, edited by Constantine Stephanidis, Margherita Antona, Stavroula Ntoa and Gavriel Salvendy
45. CCIS 1834, HCI International 2023 Posters - Part III, edited by Constantine Stephanidis, Margherita Antona, Stavroula Ntoa and Gavriel Salvendy
46. CCIS 1835, HCI International 2023 Posters - Part IV, edited by Constantine Stephanidis, Margherita Antona, Stavroula Ntoa and Gavriel Salvendy

47. CCIS 1836, HCI International 2023 Posters - Part V, edited by Constantine Stephanidis, Margherita Antona, Stavroula Ntoa and Gavriel Salvendy

https://2023.hci.international/proceedings

Preface

The cybersecurity field, in all its dimensions, is exponentially growing, evolving and expanding. New security risks emerge continuously with the steady increase of internet interconnections and the development of the Internet of Things. Cyberattacks endanger individuals and companies, as well as vital public services and infrastructures. Confronted with spreading and evolving cyber threats, the system and network defenses of organizations and individuals are falling behind, as they often fail to implement and effectively use basic cybersecurity and privacy practices and technologies.

The 5th International Conference on HCI for Cybersecurity, Privacy and Trust (HCI-CPT 2023), an affiliated conference of the HCI International Conference, intended to help, promote and encourage research in this field by providing a forum for interaction and exchanges among researchers, academics and practitioners in the fields of HCI and cyber security. The conference focused on HCI principles, methods and tools in order to address the numerous and complex threats which put at risk computer-mediated human activities in today's society, which is progressively becoming more intertwined with and dependent on interactive technologies.

In this regard, and motivated by recent worldwide developments driven by the ongoing pandemic, such as increased usage of internet and IoT services for remote working, education, shopping and health management, papers accepted in this year's proceedings emphasize issues related to user privacy and data protection. Furthermore, they focus on the usability of solutions in the field, as well as on user-centred perspectives on security and privacy.

One volume of the HCII 2023 proceedings is dedicated to this year's edition of the HCI-CPT Conference and focuses on topics related to usable security and privacy, data privacy, sovereignty and governance, cybersecurity challenges and approaches for critical infrastructure and emerging technologies, user-centered perspectives on privacy and security in digital environments, as well as human-centric cybersecurity: from intrabody signals to incident management.

Papers of this volume are included for publication after a minimum of two single–blind reviews from the members of the HCI-CPT Program Board or, in some cases, from members of the Program Boards of other affiliated conferences. I would like to thank all of them for their invaluable contribution, support and efforts.

July 2023 Abbas Moallem

5th International Conference on HCI for Cybersecurity, Privacy and Trust (HCI-CPT 2023)

Program Board Chair: **Abbas Moallem**, *San José State University, USA*

Program Board:

- Aisha Ali-Gombe, *Louisiana State University, USA*
- Mohd Anwar, *North Carolina A&T State University, USA*
- Joyram Chakraborty, *Towson University, USA*
- Ulku Clark, *University of North Carolina Wilmington, USA*
- Francisco Corella, *Pomcor, USA*
- April Edwards, *USA Naval Academy, USA*
- Ana Ferreira, *CINTESIS, Portugal*
- Steven Furnell, *University of Nottingham, UK*
- Anteneh Girma, *University of the District of Columbia, USA*
- Florian Kammüller, *Middlesex University London, UK*
- Akira Kanaoka, *Toho University, Japan*
- Mazaher Kianpour, *Norwegian University of Science and Technology (NTNU), Norway*
- Nathan Lau, *Virginia Tech, USA*
- Luca Mazzola, *HSLU - Lucerne University of Applied Sciences and Arts, Switzerland*
- Heather Molyneaux, *National Research Council Canada, Canada*
- Calvin Nobles, *Illinois Institute of Technology, USA*
- Jason R. C. Nurse, *University of Kent, UK*
- Henrich C. Pöhls, *University of Passau, Germany*
- David Schuster, *San José State University, USA*
- Arash Shaghaghi, *University of New South Wales (UNSW Sydney), Australia*
- David Stevens, *University of Hawai'i, USA*
- Adam Wójtowicz, *Poznan University of Economics and Business, Poland*
- Daniel Wilusz, *Poznan University of Economics and Business, Poland*

The full list with the Program Board Chairs and the members of the Program Boards of all thematic areas and affiliated conferences of HCII2023 is available online at:

http://www.hci.international/board-members-2023.php

HCI International 2024 Conference

The 26th International Conference on Human-Computer Interaction, HCI International 2024, will be held jointly with the affiliated conferences at the Washington Hilton Hotel, Washington, DC, USA, June 29 – July 4, 2024. It will cover a broad spectrum of themes related to Human-Computer Interaction, including theoretical issues, methods, tools, processes, and case studies in HCI design, as well as novel interaction techniques, interfaces, and applications. The proceedings will be published by Springer. More information will be made available on the conference website: http://2024.hci.international/.

General Chair
Prof. Constantine Stephanidis
University of Crete and ICS-FORTH
Heraklion, Crete, Greece
Email: general_chair@hcii2024.org

https://2024.hci.international/

Contents

Human-Centric Cybersecurity: From Intrabody Signals to Incident Management

Human-Centric Machine Learning: The Role of Users in the Development of IoT Device Identification and Vulnerability Assessment

Priscilla Kyei Danso[1(✉)], Heather Molyneaux[2], Alireza Zohourian[1], Euclides Carlos Pinto Neto[1], Derrick Whalen[3], Sajjad Dadkhah[1], and Ali A. Ghorbani[1]

[1] Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada
{priscilla.danso,alireza.zohourian,e.neto,sdadkhah,ghorbani}@unb.ca
[2] National Research Council (NRC), Fredericton, NB, Canada
heather.molyneaux@nrc-cnrc.gc.ca
[3] Information Technology Services, Port of Halifax, Halifax, NS, Canada
dwhalen@portofhalifax.ca

Abstract. Big data, Artificial Intelligence (AI), and Machine Learning (ML) have recently been posited as both a challenge and an opportunity for Human-Computer Interaction (HCI) research. Researchers and practitioners have also expressed concern about these systems' potential for favouritism, lack of transparency, and impartiality. We focus on the real-world utilization of various IoT devices and systems, communications technologies, and privacy and security considerations specific to the industry. We found that while the survey responses did validate some of our initial assumptions about privacy and security needs at Canadian ports, responses to the survey questions on IoT device and system usage and privacy and security needs were diverse, indicating an initial requirement for flexibility in UX design.

Keywords: Human-Computer Interaction · Machine Learning · Internet of Things · Security

1 Introduction

Recent literature on ethical issues surrounding AI systems shows a need for HCI research to bridge the gap between AI and HCI. Static recommendation models used by recommender systems are a quintessential example of a situation where the issue of "what precisely does a user like?" and "why does a user like this item?" are left unanswered [1]. These models are frequently employed to provide consumers with online services after being trained offline using data on past

A. A. Ghorbani—These authors contributed equally to this work.

A. Moallem (Ed.): HCII 2023, LNCS 14045, pp. 622–642, 2023.
https://doi.org/10.1007/978-3-031-35822-7_40

behaviour. Including societal norms and human values in AI systems could help address the biases in AI development and application [2].

Internet of Things (IoT) devices, can become entry points into critical infrastructure and be exploited to leak sensitive information [3]. In particular, ports are hubs for global supply chains connecting numerous operators, carriers and authorities and are particularly vulnerable to cyberattacks due to their reliance on information and communication technologies [4]. These interconnected systems operate with minimal consideration for cybersecurity risks [5]. The complexities of their ICT systems, with IoT devices, and their critical role as ports of entry into Canada make ports high risk for cybersecurity attacks, which could severely impact this country's economy and even National security [4]. The main goal of this research is to address this research challenge through device profiling, identification, intrusion detection and visualization while including end user feedback.

Our work involves training multiple Machine Learning (ML) algorithms to profile devices, identify vulnerabilities and communicate these issues with the end users. Our initial work is mainly focused on experiments with ML algorithms and standardizing data from reputable vulnerability databases tracking IoT vulnerabilities. In parallel with these activities, we have also been employing Human-Computer Interaction (HCI) methods in the system development and early stages of design using several methods. Firstly we recruited and are continuously working with an Expert by Experience (EBE) to discuss current issues in the field and validate our research directions. As a natural extension of this work, we collaborated with our EBE. We created a survey to elicit feedback from others within the industry to provide us with additional context to direct our research development.

HCI research is interested in how individuals interact with complicated systems, how to build tools and spaces for people to utilize, and how to create secure and comfortable systems and environments for the end user [6]. We employ ML techniques for IoT device profiling and identification. The development of ML systems that are dependable, credible, and realistic necessitates that pertinent interested parties, including developers, users, and subsequently the individuals who are directly impacted by these systems, get involved in the machine learning lifecycle [7]. Thus, to steer our research study in the right direction, the EBE is included to gather their perspectives on the various devices used in the ports, the technologies used at the ports, real-world experience, and other pertinent information.

This paper introduces and presents the findings of our survey. In particular, we focus on the real-world utilization of various IoT devices and systems, communications technologies, and privacy and security considerations specific to the industry. We found that while the survey responses did validate some of our initial assumptions about privacy and security needs at Canadian ports, answers to the survey questions on IoT device and system usage and privacy and security needs were diverse, indicating an initial condition for flexibility in UX design. These findings will be considered in the further refinement of our device

profiling, identification, intrusion detection, and visualization research, and we also plan to test our proof of concept and initial UX design with the end users in our future work to elicit feedback further to incorporate into our development and design cycle.

2 Background

Internet of Things (IoT) is the new technological paradigm revolutionizing operations by improving efficiency, and automation [8]. IoT devices have been employed in different sectors and industries, including but not limited to retail, healthcare, industries, cities, ports, and buildings [9]. With the emergence of IoT, ports are gradually transitioning from more traditional approaches to operation [9]. With the concept of smart ports connected to smart cities, many ports are working towards enhancing performance and fostering entrepreneurial engagement between various relevant parties to accomplish horizontal and vertical supply chain convergence [10]. The fundamental idea behind the Internet of Things (IoT) is the interconnection of many "things" with the capacity to interchange and collect their data [11], as well as the simultaneous analysis of the acquired data to disclose insights and recommend actions that result in cost savings and increased efficiency [12]. The fundamental idea of the smart port is a seamless interconnection with its surroundings and industry stakeholders, in addition to other ports and logistics players worldwide, via a communications network [10]. These "things" in IoT are employed in smart ports and are comprised mostly of devices from different manufacturers with different communication, connection protocols, and applications [13]. Such heterogeneity presents security issues such as interoperability [13] and a need for unique device identification and profiling [14].

2.1 Current Security and Privacy Challenges in IoT

The proliferation of IoT devices and the potential permanence of their usage in every facet of our lives, coupled with their heterogeneity, makes them subject to different cyberattacks. IoT security solutions must defend against risks exclusive to traditional networking and enable safe and dependable communication for both kinds of human-device interactions [15]. Since IoT is a progression of the conventional, unencrypted Internet framework, where connectivity combining the digital and physical worlds converge, security is of utmost importance [16]. Below we highlight some critical privacy and security issues facing the Internet of Things.

2.1.1 Security Challenges

We outline the significant security challenges associated with implementing IoT in the port environments because it is the foundation for smart ports.

- **Object Identification and Locating in IoT:** Before other security concerns, identifying an object is the most crucial issue. The port's extensive array of tools and equipment require unique identification in case of an anomaly of the affected object. An effective item identification process highlights the object's characteristics while also identifying the object uniquely. A host can be uniquely identified on the Internet using a Domain Name System (DNS), a reliable identifying method. It is still susceptible to man-in-the-middle, and DNS cache poisoning attacks, among other types of attacks [17].
- **Continuous Availability:** It is risky for IoT platforms to continuously protect against constant and repetitive attacks like Denial of Service (DOS) attacks since they may influence the overall core ecosystem of reliant systems [18]. Making sure IoT services are available and ongoing while preventing any possible performance breakdowns and disruptions is the primary problem.
- **Authentication and Authorization:** Traditional authentication and authorization techniques such as public-key cryptosystems and id or password might not be appropriate for IoT devices, and networks due to their heterogeneity and complexity [17]. In the case of public-key cryptosystems, managing keys could become challenging due to the continually expanding number of devices. Hence, an attacker may use weak authentication techniques to append and impersonate rogue nodes or tamper with data integrity, invading IoT devices and network connections. In these situations, there is also a constant risk that the transferred and used authentication keys will be misplaced, destroyed, or tampered with.
- **Insufficient Physical Security:** Most IoT devices run on their own in unsupervised contexts [19]. With little effort, a malicious actor may easily gain physical access to such devices without authorization and then take over. As a result, the devices would then sustain physical damage from an attacker, who might also reveal the cryptographic techniques used, duplicate their firmware using a malicious node, or corrupt their control or data [20].

2.1.2 Privacy Challenges

IoT systems gather data that may be confidential to the ports, stakeholders or personal to a user. The following must be managed more effectively during implementation:

- **Transparency and the Ethics of Data Collection:** Due to the volume of information available in potentially complicated IoT ecosystems and the discreet techniques of data gathering, users are unaware of the data practices of IoT devices and their makers [21]. Personal information could be at risk due to the increased prevalence of linked devices. The widespread usage of equipment and networks with lax security postures contributes to some threats. The primary concern with the data collected is who will have access to it and how it will be used [22].
- **Massive Data Generation:** IoT devices are producing enormous data. While IoT tracking entails tracking a device, the goal is to comprehend the

behavioural patterns of the person using the device. The wealth of knowledge about the person, their actions, movements, and preferences give that information its value. Additionally, persistent patterns of location data associated with a certain device may provide insight into that device's position at specific times of day, ultimately revealing sensitive information such as the user's workplace or home [22].

- **Privacy Regulatory and Compliance Requirements:** The utilization of numerous networks, sensors, objects, and applications, along with the worldwide nature of IoT devices, have dramatically expanded this difficulty. As a result, data may be gathered, analyzed, evaluated, and utilized across numerous jurisdictions with various laws and regulations.

2.2 Current Solutions Proposed to Address the Security and Privacy Challenges in IoT

There are several security and privacy challenges in IoT. These include fixed access control, the challenge of building a standard system for various IoT devices, managing mass amounts of heterogeneous data, and the inherent resource limitations of IoT devices. Researchers are addressing these issues in multiple forms.

To address the fixed access control technique applied to privilege management and how interdependent actions affect IoT security [23], Jia et al. [24] proposed ContextIoT - a context-based authorization system for applied IoT systems that supports fine-grained contextual recognition for critical operations and runtime signals with rich content delivers contextual coherence.

It is challenging to build a standard defence system for heterogeneous devices because of the diversity of IoT devices, especially in industrial sectors [25] like smart ports. Therefore, it is vital to address how to find and solve the numerous security flaws present among the various IoT devices. Because each protocol differs from the others in terms of network security, researchers need to identify their most significant generic security flaws. Additionally, researchers should consider the security issues with a single protocol and any possible security threats linked to other protocols [23].

To address the issue of heterogeneity on the hardware level, Davidson et al. [26] designed and implemented an automated security analysis tool to provide an extensible platform for detecting bugs in firmware programs for some of the popular families of microcontrollers. The goal of the proposed solution by the authors is to verify the security properties of the simple firmware often found in practice.

Researchers are also addressing the issue of massive and heterogeneous data management. Li et al. proposed a storage management solution based on NoSQL called IOTMDS [27]. NoSQL systems provide high availability and performance. This study aims to delve into how to efficiently and intelligently store large amounts of IoT data while simultaneously looking out for data collaboration and exchange amongst various IoT apps. To enhance cluster performance and

efficiently store data, two data preparation procedures were suggested in the design.

Most IoT devices do not deploy the essential defence mechanisms for the system and network because of the resource limitations of the IoT. Zhao et al. created and developed a lightweight solution that employs software fault isolation to redesign a compiled program and include a dynamic inspection before each risky action to improve system security for restricted IoT devices [28]. The intended outcome of the suggested approach is to offer an extreme case that its storage security and control flow trustworthiness standards are not broken and that devices may be trusted. Attacks on IoT devices are varied because of their heterogeneity and lack of appropriate security defences. Finding ways to recognize and defend against various attacks on IoT devices, such as a bonnet, Denial of Service (DoS), or Distributed Denial of Service (DDoS), is now a major challenge. Furthermore, how to detect these attacks is the difficult challenge at hand. However, McDermott et al. [29] offer a method for identifying botnet activity in IoT networks and consumer devices. A Deep, Bidirectional Long, Short Term, Memory based Recurrent Neural Network, was used to create a detection model (BLSTM-RNN). At the packet level, the detection was carried out with an emphasis on text recognition inside characteristics that conventional flow-based detection techniques would often overlook. The accuracy and loss are evaluated.

Device profiling and identification have emerged as a cutting-edge strategy that considerably reduces some, but not all, of the security concerns in IoT devices. The fingerprinting of a device is one of the well-known methods for device identification. The majority of the time, using device network traffic or physical properties, and behavioural patterns, there are numerous techniques to fingerprint the device. Similar to user authentication, device identification validates the legitimacy of the attached device to the network [30]. Due to the heterogeneity of the IoT ecosystem, accurate device identification is necessary but also challenging. Device identification describes a method that determines an IoT device based on its features. Cui et al. [31] described IoT device identification: *the input is various data collected from a device, e.g. sensors' data, network data, etc.; the output is a label for the IoT device indicating the type of the device.*

The five device identification techniques identified during our literature review are Fingerprinting, Machine Learning, Deep Learning, Manufacturer Usage Description (MUD), and Blockchain in Fig. 1. We review the works of different researchers for each identification technique.

Locality-sensitive IoT fingerprinting (LSIF), a unique method for identifying IoT devices, is presented by Charyyev et al. [32]. A locality-sensitive hash (LSH) function called Nilsimsa is used to construct the traffic profile of an IoT device from the flow of its network traffic. A signature database is then used to hold the relevant device target variable and produce a hash set. The highest average hash similarity score between each recorded device and the device being identified is

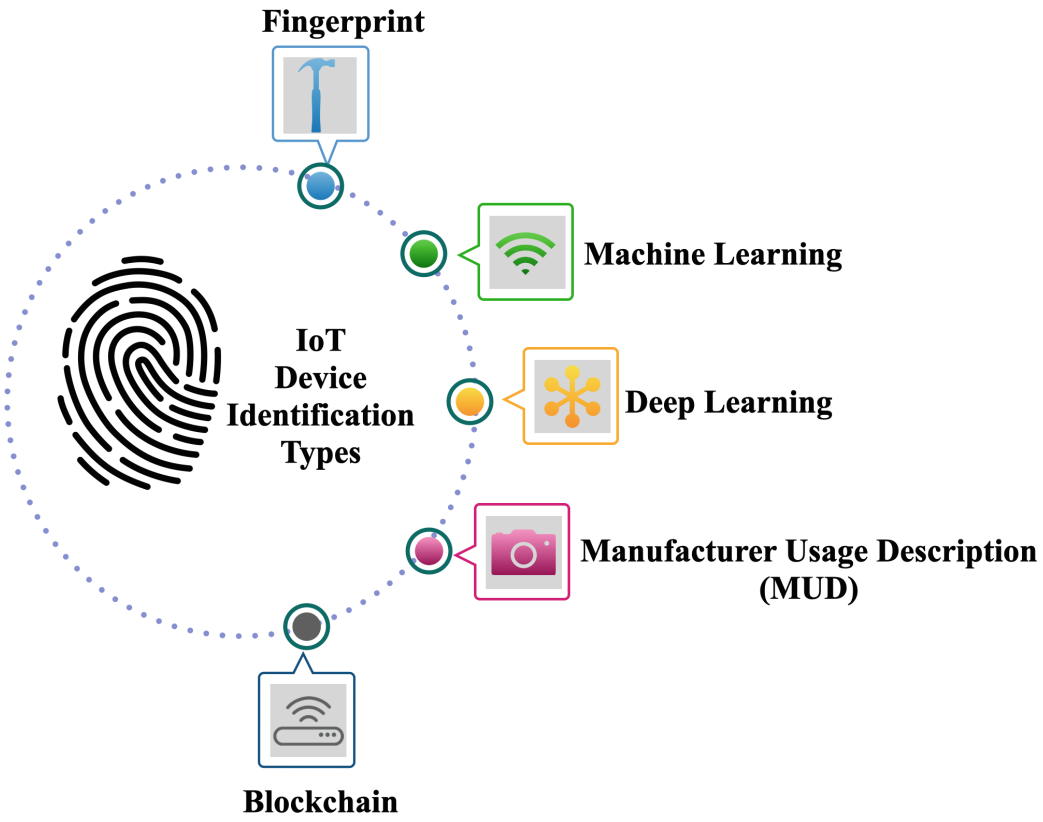

Fig. 1. IoT Identification Approaches.

computed. A comparison is made on the LSH of a new device joining the network and the hash values previously stored in the database.

To identify unauthorized IoT devices connected to a network, Yair et al. [33] used TCP/IP traffic network data for categorization by ML. The authors assume that the dataset adequately reflected each device type on the whitelist. To effectively identify IoT device types from the allowlist, features from network traffic data were extracted using supervised machine learning, especially Random Forest. Nine IoT device categories totaling 17 unique IoT devices were gathered and manually labeled to train and test multi-class classifiers. The trained classifiers obtained an average of 96% accuracy in detecting illegitimate IoT device types.

Jaidip et al. [34] detected IoT devices linked to a network using data from traffic data, precisely IoT devices not on the whitelist (unknown devices) using a deep learning approach. The method the authors suggested was based on representation learning and consisted of two experiments: one for detecting legitimate IoT devices in network traffic and the second for identifying illegitimate devices attached to a network. The proposed method identified known devices in a network with a maximum accuracy of 99.87% (Table 1).

Alam et al. [35] proposed a generalized fingerprinting approach based on blockchain technology to authenticate edge devices with distinctive PUF IDs (Physical Unclonable Function Identifications embedded in the device's memory

Table 1. Summary of device profiling and identification review. ML, F, DL, BC, and MUD each represent the different approaches used in the profiling and identification of a device Machine Learning, Fingerprinting, Deep Learning, Blockchain and Manufacturer Usage Description respectively.

No	Paper	Purpose	Algorithm/Tools	Type of Identification
1	[32]	IoT device identification using locality-sensitive hash (LSH) function	LSH function called Nilsimsa	F
2	[33]	Identify unauthorized IoT devices connected to a network	Random Forests (RF)	ML
3	[34]	Detect IoT devices in a network using data from traffic data	Neural Network	DL
4	[35]	Authenticate edge devices	Blockchain ledger BL	BC
5	[30]	IoT device profiling	Manufacturer Usage Description (MUD)	MUD

during production). They distinguish between a global and local component. While the global system verifies registered devices by anybody, anywhere, without being able to pinpoint the particular manufacturer, the local implementation allows defence-in-depth authenticity. The device identification is verified after a thorough approval process in which hashed values of both the blockchain ledger BL and gateway coincide.

Manufacturer Usage Description (MUD) [36] is a new standard created by the Internet Engineering Task Force (IETF). The MUD specification defines device profiles. An IoT device will submit a MUD URL along with its LLDP, DHCP, or X.509 request [30] when it initially joins an access control station. The MUD Manager converts this conceptual goal into a context-specific guideline and sent to the server. The server then enacts the policies on the network utilizing Access Control Lists (ACLs) for that IoT device's entry outlet. Then, depending on the maker's predetermined goal, accessibility to the device is granted.

3 Our Proposed System

The three primary components of the proposed framework are the device identification and profile, vulnerability analysis, and visualization or dashboard module. The primary motivation behind the proposed architecture is to have a compound system responsible for utilizing Machine Learning to detect the device type in a network while also evaluating and displaying their vulnerabilities. Although there are a number of processes that each component in the proposed system must go through, the work of Dadkhah et al. [14] provides a detailed explanation of these procedures. The surveys from the EBEs in our study were also used to evaluate our preliminary project findings and to highlight user interest areas that would be included in the final system design (Fig. 2).

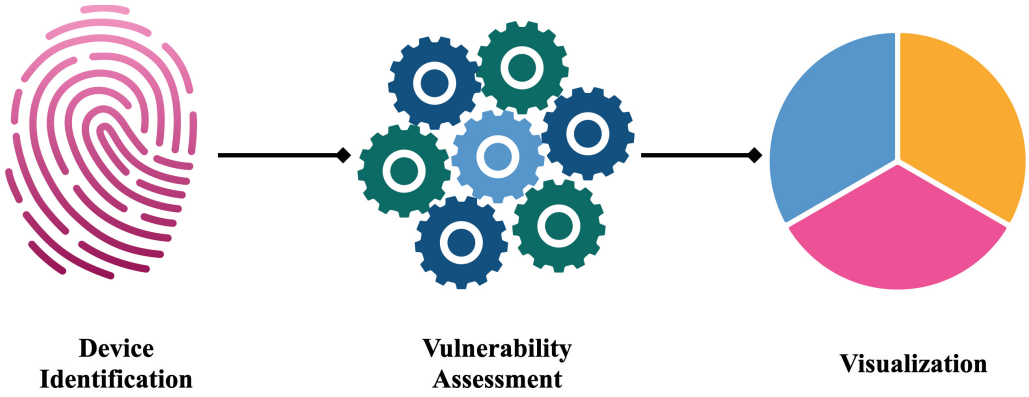

Fig. 2. System Flow.

4 Methodology

The first step to address this research challenge is to identify state-of-the-art IoT and logistics for the industry by investigating the most effective and commonly used devices, the resulting raw data, and possible attack threats. Initially, a literature review was undertaken, and findings were presented in an internal report; however, this search revealed little about the specific details of the devices used in the ports, technologies used at the ports, and the real-world experience. In order to understand the needs of operators at Port authorities as well as the devices commonly used within ports, we developed a survey whereby IT experts at the ports were asked to provide feedback on survey questions related to the current and future IoT needs, as well as devices used at the port. The survey was informed by our previous literature searches and was created with input and feedback from our EBE at the Port of Halifax. Participation was voluntary, and the survey was approved by NRC's Research Ethics Board (REB). In April, surveys were sent out via email to Port authorities with one reminder email. Eight port authorities were contacted by one researcher (including the five most important ports in Canada and three additional ports), and our EBE and four port authority representatives completed the survey. Data collection ended in August.

4.1 Demographics

From the survey responses, we can determine that most of the ports were medium-sized ports, employing 51–100 people. One larger-sized port, employing 201–300 people, filled out the survey (Fig. 3).

Responses to the question on how many IoT devices the ports currently have were varied, with two ports noting currently having between 0–500 IoT devices, one port having between 501–1000 devices and one port having more than 1000 (Fig. 4).

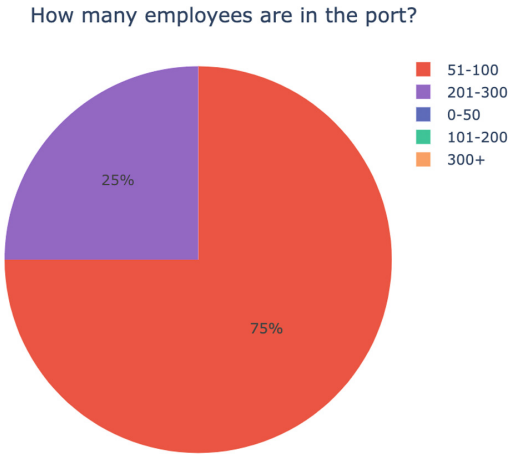

Fig. 3. Number of employees.

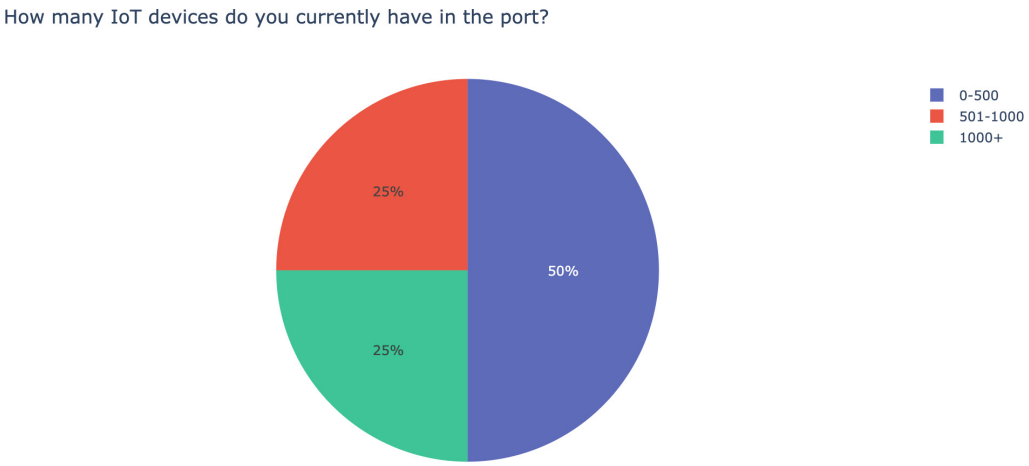

Fig. 4. Number of IoT devices.

Most of the ports reported high rates of implementing and considering privacy and security concerns in their current configurations (Fig. 5), with one exception discussed in more detail in the next section of this report.

Likewise, most of the ports also noted implementing and considering the use of monitoring, profiling, and tracking (Fig. 6), with one exception that is discussed in more detail in the next section of this report.

When asked which performance measures were significant, the accuracy of estimation and greenhouse gas emissions were the two most important performance measures to the ports (Fig. 7). In the written comments of the survey, two of the four ports noted that bandwidth for remote IoT and/or video devices could be a performance issue in their configuration. The largest port (P3) reported no problems with its configuration and rated all performance measures as 4 or 5.

All ports reported using cameras, sensors, and office accessories (Fig. 8). The port representatives were asked which devices they used in operations and given the ability to write in additional devices. A later question asked for more specific

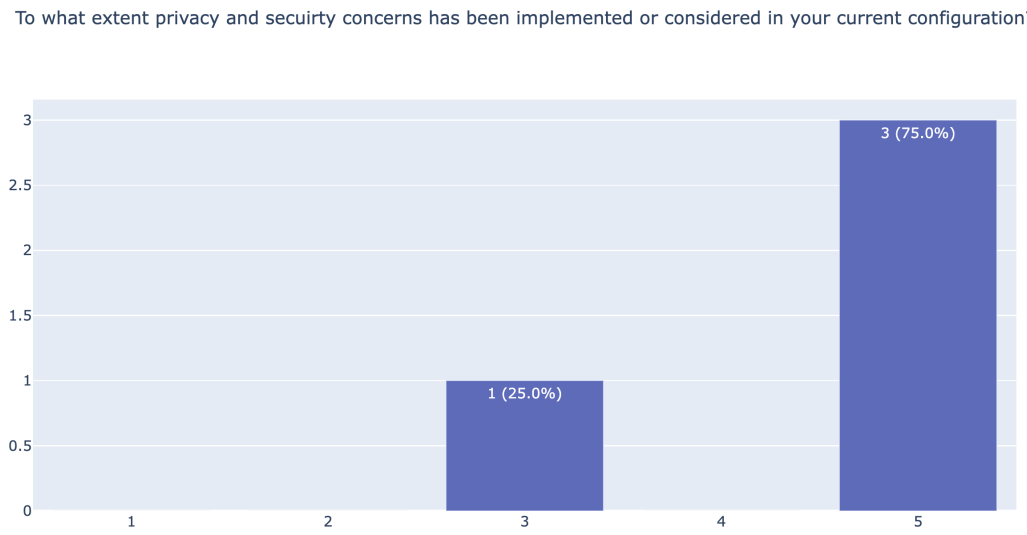

Fig. 5. Privacy and Security.

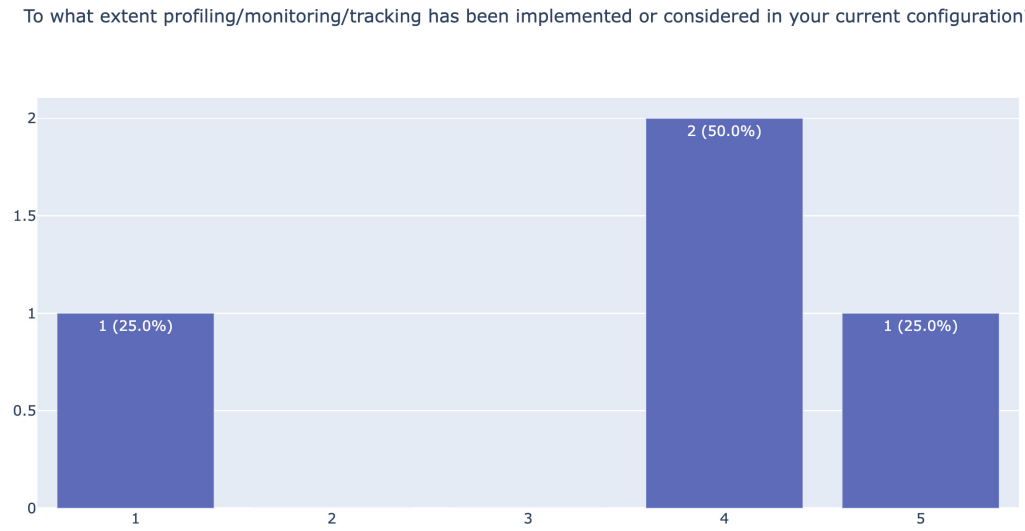

Fig. 6. Monitoring/Profiling/Tracking.

details about the types of sensors they employ at their port. One of the smaller ports noted having gates and access controls (a written response which they added).

All of the ports reported using Ethernet and 4G/5G, and most also use WiFi and RFID (Fig. 9). The largest port (P3) was the only one to report using LoRaWAN, and here they note that they do not use WiFi (which is contradictory to their response on a later question response); they also report not using GPS and Zigbee/Z-Wave.

Smart production management and smart parking lots were the two applications not employed by any of the ports surveyed (Fig. 10). Interestingly the

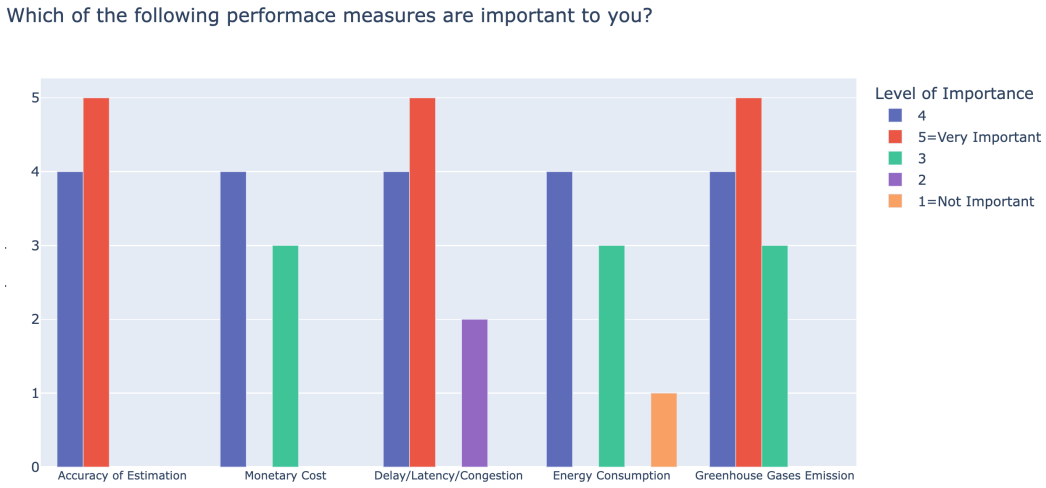

Fig. 7. Performance measures.

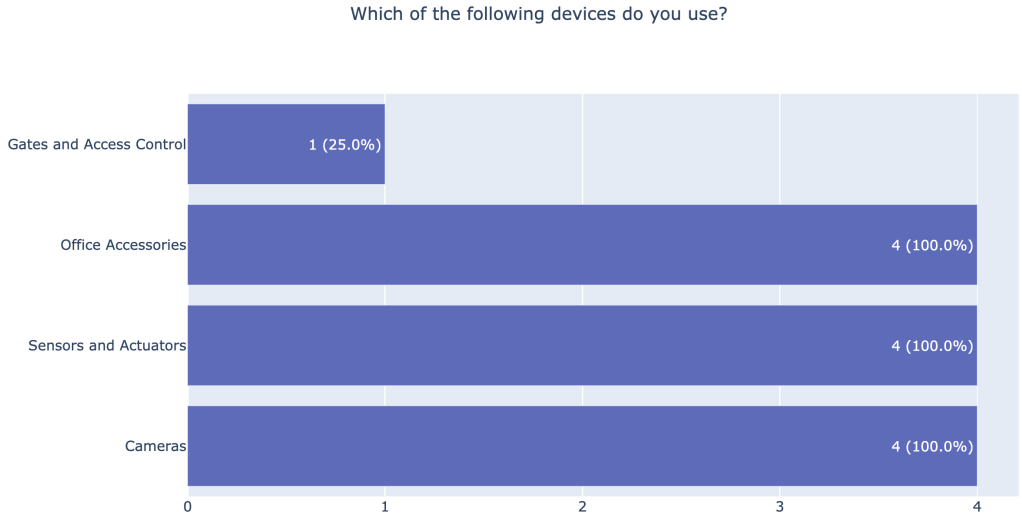

Fig. 8. Category of devices used.

largest port only reported currently operating smart operation management and Smart lighting, while one of the smaller ports reported using a greater variety of smart management systems (P1 noted using 5; P2 uses 3; P4 uses 2).

Many of the port authority representatives may know they need to expand their current usage of communication technologies. Not surprisingly, WiFi, Ethernet, RFID, and 4/5G were all required for all ports for land, and 4/5G and GPS for trucks in all four ports. Temperature, motion, image, dust, and wind sensors are currently employed in all ports (Fig. 11). There was a discrepancy between answers here with the use of LoRaWAN and an earlier question asking which communication technologies the ports currently employ (Fig. 9); however, the difference could be related to asking them which communication technologies they now use compared to which communication technologies they need.

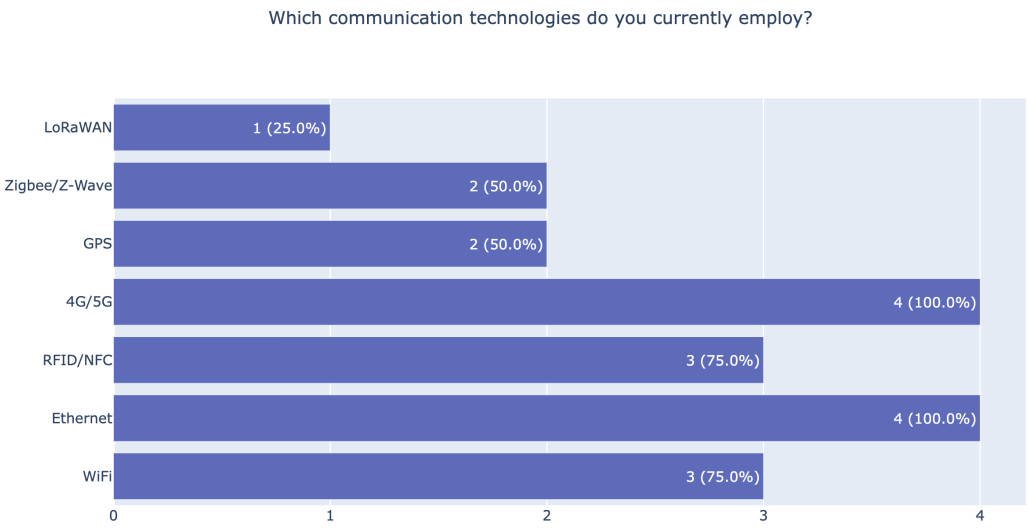

Fig. 9. Communication Technologies.

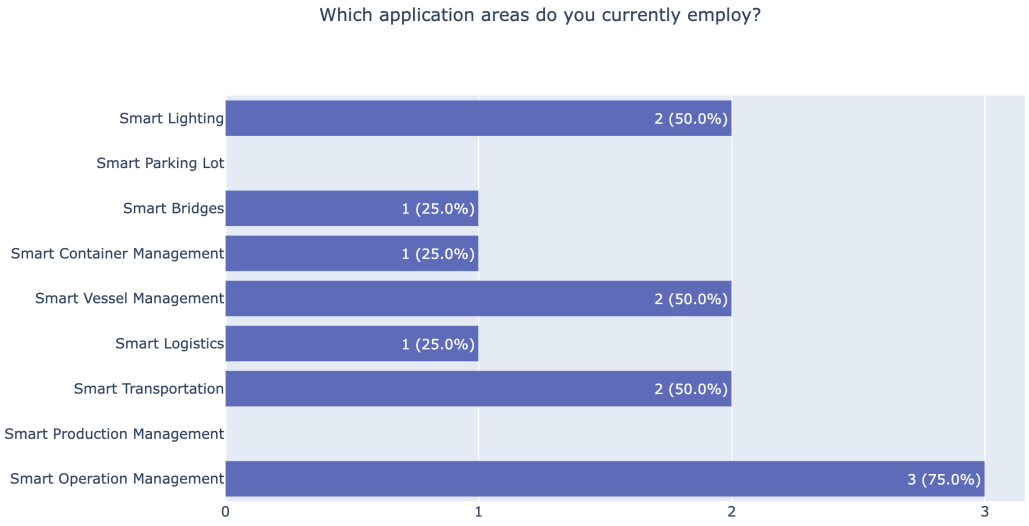

Fig. 10. Current application areas.

Temperature, motion, image, dust, and wind sensors are currently employed by all ports (Fig. 12). The largest port uses the most sensors (all but pressure, water, and gyroscopic sensors), but the smaller ports also employ many of the sensing systems; for example, P1 uses all sensing systems listed except water quality, chemical, acceleration, and gyroscopic sensors. P1 also wrote that they use water current sensors.

Not many ports currently use LoRaWAN, as we saw in Fig. 9; however, there is a need for it, especially for trucks and rail applications (Fig. 11), and here in Fig. 13 the majority of the respondents note an interest in employing and/or extending their use of the technology. Other technologies of note include WiFi, Ethernet, GPS, and, to a lesser extent, 4G/5G.

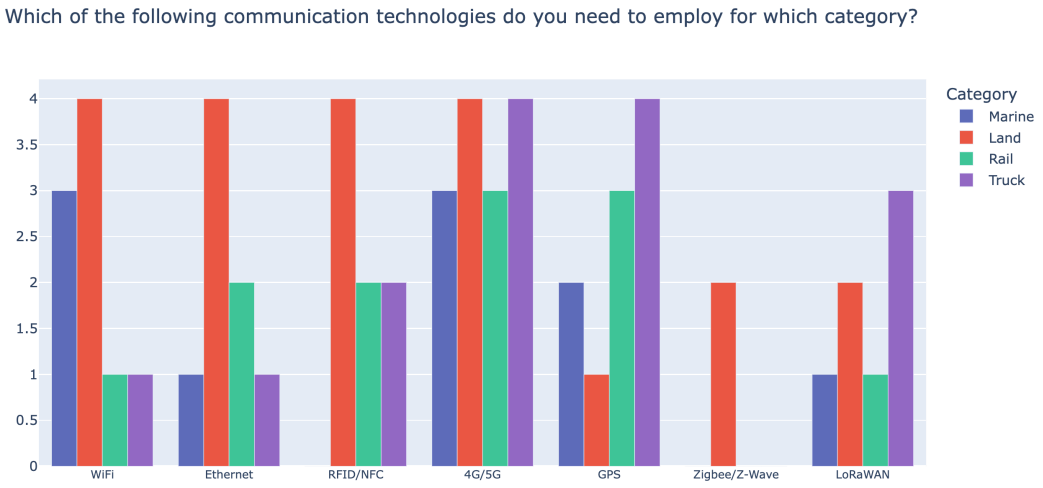

Fig. 11. Communication Technologies needed.

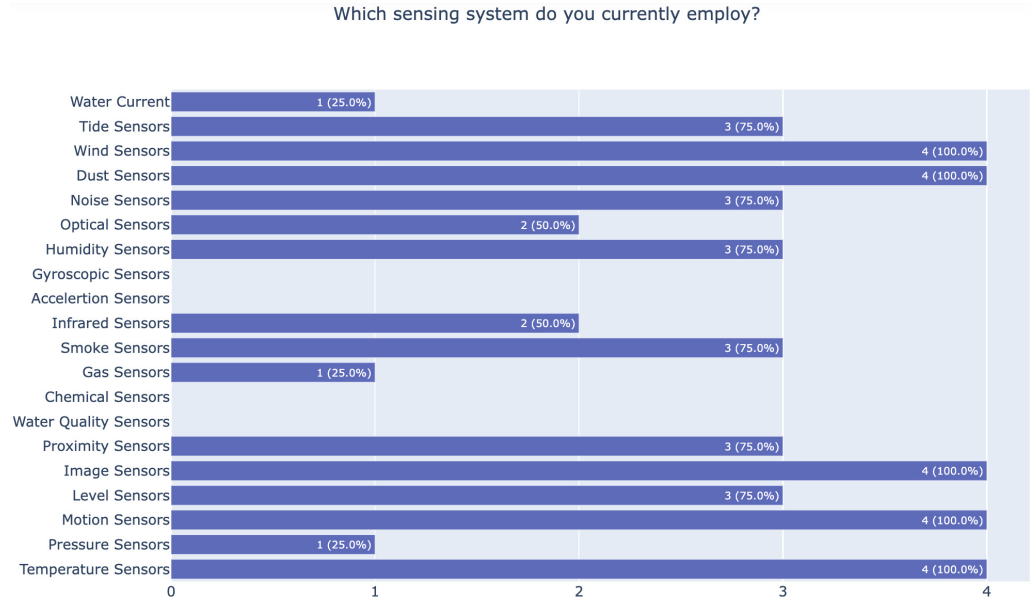

Fig. 12. Current sensing systems.

Smart transportation was noted as the number one application area of interest for employing or extending, followed by smart operation management (which three ports already use - Fig. 10), smart container management, and smart lighting (Fig. 14). While the most prominent port (P3) reported only using two application areas currently, they reported being very interested in all of the application areas listed, except for smart bridges and parking lots (marked "a little interested").

Most ports showed interest in employing and/or extending their image, dust, and wind sensor systems. All were interested in water quality sensors (Fig. 15). The ports had different responses to this question based on many factors, includ-

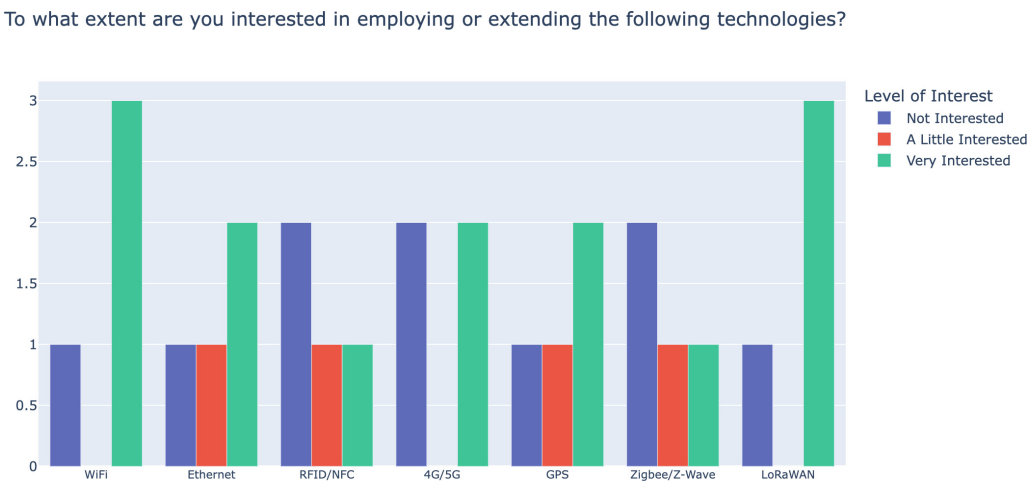

Fig. 13. Interest in communication technologies.

Fig. 14. Interest in application areas.

ing their current use of sensor systems, which will be detailed in the discussion section.

The port authorities were also asked which types of sensing systems were needed for which category: marine, land, rail, and trucks. All four ports reported needing temperature, motion, humidity, noise, dust, and wind sensors for land. Image sensors were reported as necessary for all aspects of operations within the port (marine, ground, rail, and truck); wind sensors were reported by 3 of the four ports as needed for marine operations; noise sensors were reported from 3 of the four ports as also required for marine, rail, and trucks. Three of the four ports reported needing tide sensors (which could indicate the difference between ocean ports and those located on lakes or rivers) (Fig. 16).

Fig. 15. Interest in employing/extending sensing systems.

Fig. 16. Sensing systems for categories.

The responses from the ports to most of the survey questions were diverse. These differences are further investigated in the next section.

5 Discussion

The ports surveyed had varying responses to the survey questions. Some of these differences were related to the size of the port. For example, the largest port (P3) reported the highest number of employees (300+) (Fig. 3) and IoT devices (1000+) (Fig. 4). The largest port also employs a broader variety of sensor types than the other ports (Fig. 12). For example, one of the smaller ports (using 51–100 people) reported having a large number of IoT devices (over 500) (P1). Also, the smaller ports indicated that they use more smart management systems than the more critical port (with P1 noting they are using 5; P2 uses 3; and P4 uses 2 - the same number as the more critical port) (Fig. 10). Therefore it would be unwise to assume that ports employing fewer people use fewer IoT devices automatically. However, it would be wrong to assume that large ports are the only ones interested in IoT.

The port size was not a predictor of the port interest in employing/extending technologies (Fig. 13). The large port noted they were very interested in most technologies and a little in Ethernet, GPS, and Zigbee (P3). Likewise, one of the smaller ports responded similarly to the larger port, expressing interest in all the technologies aside from RFID (which they note they were a little interested in) (P2); however, P1 reported only being very interested in Zigbee, and P4 was only very interested in WiFi and Ethernet. Both P1 and P4 checked that they were not interested in the other communication technologies.

Likewise, low levels of interest in employing new or extending current sensing systems in Fig. 13 doesn't mean that the ports aren't interested at all in sensors - for example, P1 reported using all sensors except water quality, chemical, acceleration, and gyroscopic sensors - so they responded not interested in expanding/employing sensors for most of the sensors, excluding image, [proximity, water quality, noise, dust, wind, and tide sensors, which they noted is a little interested in P2, which reported using fewer sensors than P1 and P4, states that they were interested in expanding or adopting the motion, image, noise, dust, wind, and tide sensor systems. The large port, which uses the most sensors, noted that they were interested in employing or extending all sensor systems except pressure, water quality, and gyroscopic (which they said is a little interested in) (P3). P4, another more minor port with fewer sensor systems, noted that they were interested in image, dust, and wind sensors. All four ports answered this question very differently, but from the responses, we see a clear need for the use and extended use of image, dust, and wind sensor systems in particular (Fig. 15). The use of image sensors, in particular, is of great importance, as all four ports noted needing image sensors for marine, land, rail, and truck operations within the port (Fig. 16).

It would also be a false assumption to categorize larger and smaller ports as having different attitudes toward privacy and security. The largest port (P3)

ranked privacy and security considerations and implementation as the highest consideration (5) and monitoring/profiling/tracking as the high consideration (4). Meanwhile, one more minor port noted privacy and security are of the highest consideration (5) and that they also highly implement/consider monitoring/profiling and tracking (5). This was the same port that reported having over 500 IoT devices (P1), which indicates they know they need to be aware and concerned about privacy and security within the port. They acknowledge the importance of monitoring, profiling, and tracking IoT devices. Similarly, another smaller port (P4) considered privacy and security highly assumed (5), and monitoring, profiling, and tacking were also considered (4).

However, not all of the responses about privacy and security from the ports were the same. One of the smaller ports (P2) noted that monitoring/tracking/profiling is not being considered (1); the same more minor port noted privacy and security concerns are not believed in the current configuration (answering "3" in the Likert scale).

The responses from P2 do not necessarily indicate that they are not interested in or aware of privacy and security concerns. Perhaps they suggest that they know that their port needs to do more. Their responses to the survey indicate they are interested in IoT solutions at their dock. The same port representative wrote in the study about having IoT for gates and access control, bandwidth challenges for video, smart operations management, smart transportation, and smart bridges. They also indicated that they are very interested in including or expanding upon in the future the port's smart operation management, smart transportation, smart vessel management, smart container management, smart bridges, and smart lighting (P2). Currently, P2 employs WiFi, Ethernet, 4G/5G, and Zigbee/Z-Wave. It is very interested in all technologies except RFID (which they indicated that they were a little interested in) P2 also currently employs various sensors such as temperature, motion, image, proximity, noise, dust, wind, and tide. They also indicated that in the future, they are interested in including and/or expanding upon motion, image, proximity, noise, dust, wind, and tide sensors. To further the conclusion that P2 is interested in growing their use of IoT, their final comment in the survey is that: "IoT solutions expected to grow in future" (P2).

6 Conclusions

Our study mixes training ML algorithms to profile devices and identify vulnerabilities with HCI approaches to direct and validate our research directions. Through our HCI work, we validated the importance of privacy and security at the ports and the priority, in particular, of image sensor systems. Several findings from the survey will inform our design outcomes, such as the importance of specific types of sensors and systems and the need for flexibility in UX design, as survey responses showed the diversity of the types of devices and systems used in the various ports. Questions related to the current and future IoT use in the ports support the idea of the growth in IoT at the ports and the need to support this growth with mindful privacy and security measures.

There are several limitations to our study. Our work was conducted during the Covid-19 pandemic, which limited our use of user studies. Meetings with the EBE were all conducted remotely, and the survey was administered online. Our survey contains a small sample size but within a relatively small population size, as there are only 17 Canadian Port Authorities recognized as such due to their strategic importance. Future work will involve engaging the EBE and other users for UX design and feedback through a cognitive walkthrough of the prototype.

Acknowledgments. The authors graciously acknowledge the support from the Canadian Institute for Cybersecurity (CIC), the funding support from the National Research Council of Canada (NRC) through the AI for Logistics collaborative program, the NSERC Discovery Grant (no. RGPIN 231074), and Tier 1 Canada Research Chair Dr. Ghorbani.

References

1. Gao, C., Lei, W., He, X., de Rijke, M., Chua, T.-S.: Advances and challenges in conversational recommender systems: a survey. AI Open **2**, 100–126 (2021). https://doi.org/10.1016/j.aiopen.2021.06.002
2. Lee, M.K., et al.: Human-centered approaches to fair and responsible AI. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA 2020), pp. 1–8. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3334480.3375158
3. Rockefeller, S.: A kill chain analysis of the 2013 target data breach. Committee on Commerce, Science and Transportation, Tech. Rep. (2014)
4. Meyer-Larsen, N., Müller, R.: Enhancing the cybersecurity of port community systems. In: Freitag, M., Kotzab, H., Pannek, J. (eds.) LDIC 2018. LNL, pp. 318–323. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-74225-0_43
5. Trimble, D., Monken, J., Sand, A.F.L.: A framework for cybersecurity assessments of critical port infrastructure. In: 2017 International Conference on Cyber Conflict (CyCon U.S.), pp. 1–7 (2017). https://doi.org/10.1109/CYCONUS.2017.8167506
6. Moustakis, V.S., Herrmann, J.: Where do machine learning and human-computer interaction meet? Appl. Artif. Intell. **11**(7–8), 595–609 (1997)
7. Vaughan, J.W., Wallach, H.: A human-centered agenda for intelligible machine learning. Machines We Trust: Getting Along with Artificial Intelligence (2020)
8. Jun, W.K., Lee, M.-K., Choi, J.Y.: Impact of the smart port industry on the Korean national economy using input-output analysis. Transp. Res. A Policy Pract. **118**, 480–493 (2018). https://doi.org/10.1016/j.tra.2018.10.004
9. Yang, Y., Zhong, M., Yao, H., Yu, F., Fu, X., Postolache, O.: Internet of things for smart ports: technologies and challenges. IEEE Instrum. Meas. Mag. **21**(1), 34–43 (2018). https://doi.org/10.1109/MIM.2018.8278808
10. Philipp, R.: Digital readiness index assessment towards smart port development. Sustain. Manag. Forum — NachhaltigkeitsManagementForum **28**(1), 49–60 (2020). https://doi.org/10.1007/s00550-020-00501-5
11. Minerva, R., Biru, A., Rotondi, D.: Towards a definition of the internet of things (IoT). IEEE Internet Initiative **1**(1), 1–86 (2015)
12. Davies, R.: The internet of things: opportunities and challenges (2015)

13. Noaman, M., Khan, M.S., Abrar, M.F., Ali, S., Alvi, A., Saleem, M.A.: Challenges in integration of heterogeneous internet of things. Sci. Program. **2022**, 8626882 (2022). https://doi.org/10.1155/2022/8626882
14. Dadkhah, S., Mahdikhani, H., Danso, P.K., Zohourian, A., Truong, K.A., Ghorbani, A.A.: Towards the development of a realistic multidimensional IoT profiling dataset. In: 2022 19th Annual International Conference on Privacy, Security and Trust (PST), pp. 1–11 (2022). https://doi.org/10.1109/PST55820.2022.9851966
15. Punla, C.S., Farro, R.C.: Are we there yet?: an analysis of the competencies of BEED graduates of BPSU-DC. Int. Multidiscip. Res. J. **4**(3), 50–59 (2022)
16. Hamad, S.A., Sheng, Q.Z., Zhang, W.E., Nepal, S.: Realizing an internet of secure things: a survey on issues and enabling technologies. IEEE Commun. Surv. Tutor. **22**(2), 1372–1391 (2020). https://doi.org/10.1109/COMST.2020.2976075
17. Zhang, Z.-K., Cho, M.C.Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., Shieh, S.: Iot security: ongoing challenges and research opportunities. In: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234 (2014). https://doi.org/10.1109/SOCA.2014.58
18. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: DDoS in the IoT: Mirai and other botnets. Computer **50**(7), 80–84 (2017). https://doi.org/10.1109/MC.2017.201
19. Butun, I., Österberg, P., Song, H.: Security of the internet of things: vulnerabilities, attacks, and countermeasures. IEEE Commun. Surv. Tutor. **22**(1), 616–644 (2020). https://doi.org/10.1109/COMST.2019.2953364
20. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., Ghani, N.: Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Commun. Surv. Tutor. **21**(3), 2702–2733 (2019). https://doi.org/10.1109/COMST.2019.2910750
21. Lipford, H.R., Tabassum, M., Bahirat, P., Yao, Y., Knijnenburg, B.P.: Privacy and the internet of things. In: Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J. (eds.) Modern Socio-Technical Perspectives on Privacy, pp, 233–264. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-82786-1_11
22. Policy Group, R., et al.: The internet of things: an introduction to privacy issues with a focus on the retail and home environments. Office of the Privacy Commissioner of Canada (2016)
23. Zhou, W., Jia, Y., Peng, A., Zhang, Y., Liu, P.: The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J. **6**(2), 1606–1616 (2019). https://doi.org/10.1109/JIOT.2018.2847733
24. Jia, Y., et al.: ContexIoT: towards providing contextual integrity to appified IoT platforms. In: Network and Distributed System Security Symposium (2017)
25. Rubio-Hernan, J., Rodolfo-Mejias, J., Garcia-Alfaro, J.: Security of cyber-physical systems. In: Cuppens-Boulahia, N., Lambrinoudakis, C., Cuppens, F., Katsikas, S. (eds.) CyberICPS 2016. LNCS, vol. 10166, pp. 3–18. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-61437-3_1
26. Davidson, D., Moench, B., Ristenpart, T., Jha, S.: Fie on firmware: finding vulnerabilities in embedded systems using symbolic execution. In: USENIX Security Symposium (2013)
27. Li, T., Liu, Y., Tian, Y., Shen, S., Mao, W.: A storage solution for massive IoT data based on NoSQL. In: 2012 IEEE International Conference on Green Computing and Communications, pp. 50–57 (2012). https://doi.org/10.1109/GreenCom.2012.18

28. Zhao, L., Li, G., De Sutter, B., Regehr, J.: ARMor: fully verified software fault isolation. In: 2011 Proceedings of the Ninth ACM International Conference on Embedded Software (EMSOFT), pp. 289–298 (2011)
29. McDermott, C.D., Majdani, F., Petrovski, A.V.: Botnet detection in the internet of things using deep learning approaches. In: 2018 International Joint Conference on Neural Networks (IJCNN), pp. 1–8 (2018). https://doi.org/10.1109/IJCNN.2018.8489489
30. Mazhar, N., Salleh, R., Zeeshan, M., Hameed, M.M.: Role of device identification and manufacturer usage description in IoT security: a survey. IEEE Access **9**, 41757–41786 (2021). https://doi.org/10.1109/ACCESS.2021.3065123
31. Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N., Qin, J.: A survey on application of machine learning for Internet of Things. Int. J. Mach. Learn. Cybern. **9**(8), 1399–1417 (2018). https://doi.org/10.1007/s13042-018-0834-5
32. Charyyev, B., Gunes, M.H.: Locality-sensitive IoT network traffic fingerprinting for device identification. IEEE Internet Things J. **8**(3), 1272–1281 (2021). https://doi.org/10.1109/JIOT.2020.3035087
33. Meidan, Y., et al.: Detection of unauthorized IoT devices using machine learning techniques. arXiv preprint arXiv:1709.04647 (2017)
34. Kotak, J., Elovici, Y.: IoT device identification using deep learning. In: Herrero, Á., Cambra, C., Urda, D., Sedano, J., Quintián, H., Corchado, E. (eds.) CISIS 2019. AISC, vol. 1267, pp. 76–86. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-57805-3_8
35. Alam, S.R., Jain, S., Doriya, R.: Security threats and solutions to IoT using blockchain: a review. In: 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 268–273 (2021). https://doi.org/10.1109/ICICCS51141.2021.9432325
36. Lear, E., Droms, R., Romascanu, D.: Manufacturer usage description specification. RFC Editor (2019). https://doi.org/10.17487/RFC8520. https://www.rfc-editor.org/info/rfc8520