

# **PRIVACY, INTEGRITY AND PERFORMANCE OF EDGE DEVICES FOR SUSTAINABILITY**

**ISMI ABIDI**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
INDIAN INSTITUTE OF TECHNOLOGY DELHI**

October 2022



© Indian Institute of Technology Delhi (IITD), New Delhi, 2022



# **PRIVACY, INTEGRITY AND PERFORMANCE OF EDGE DEVICES FOR SUSTAINABILITY**

by

ISMI ABIDI

Department of Computer Science and Engineering

Submitted

in fulfillment of the requirements of the degree of **Doctor of Philosophy**

to the



**Indian Institute of Technology Delhi**

**October 2022**



# Certificate

This is to certify that the thesis titled **PRIVACY, INTEGRITY AND PERFORMANCE OF EDGE DEVICES FOR SUSTAINABILITY**, submitted by Ms. **Ismi Abidi**, to the Indian Institute of Technology, Delhi, for the award of the degree of **Doctor of Philosophy** in Computer Science & Engineering, is a record of bona fide work carried out by her under my guidance and supervision at the Department of Computer Science & Engineering, Indian Institute of Technology Delhi. The contents of this thesis, in full or in parts, have not been submitted elsewhere for the award of any degree or diploma.

**Dr Rijurekha Sen**

Assistant Professor

Dept. of Computer Science and Engineering

Indian Institute of Technology Delhi

New Delhi-110016



# Acknowledgements

*The sweetness of success erases the bitterness of patience.*

–Hazrat Ali (A.S.)

I am thankful to everybody who has contributed to the completion of my PhD thesis in their own capacity. I highly appreciate all the assistance I received during my PhD, whether it was related to infrastructure, technical, financial, or moral support.

I have no words to express my gratitude towards my advisor Dr. Rijurekha Sen, for her timely personal and professional support. I will always remember how she provided me the support when I was at the darker phases of my PhD, and the odds were against me. Her encouragement, motivation, and help in my research, while she was herself dealing with some personal tragedies, gave me a lesson of a lifetime.

I would also like to thank my collaborators Dr. Paarijaat Aditya, Dr. Vireshwar Kumar, and last but not the least Ishan Nangia, for the interesting discussions, all virtually, we had. A special thank to Nakul for helping in carrying out the initial vehicular deployments. I am very grateful to my SRC members-Prof. Huzur Saran, Dr. Subodh Sharma, and Dr. Mukul Sarkar-for serving on my committee and gracing me with their valuable feedback.

Thanks Hameedah, Diksha, and Mehreen, for the lovely tea and snack time. The list of my acknowledgment will not be complete without mentioning the names of Indu and Omais. Both of them being the source of positivity and encouragement during the difficult days of my research. I acknowledge my colleague and friend Maliha for providing me the accommodation when I desperately needed one to complete my final experiments. Finally, I would like to offer special thanks to Himanshu, who left us very early. He will continue to inspire me to be always supportive and helpful.

Last but most importantly, I express my sincere thanks to my family for their limitless love, backup, and support. I will always be grateful to my father, who lend me an ear, anywhere

and anytime. Finally, everything I achieved in my life, I owe it to my mother and father.  
*Alhamdulillah!!*

*The greatest pleasure in life is doing what people say you cannot do.*

–Walter Bagehot

**Ismi Abidi**

# Abstract

Recent times have witnessed the emergence of air pollution as one of the pressing sustainability issues. Even though it is a global issue, this problem intensifies for Delhi and NCR. Despite the intensity of this problem, there are very few air quality monitoring stations in the capital. The major roadblock in the adoption of existing solutions is high price. It has motivated us to design a low-cost scalable sensing solution for air pollution monitoring. Scalable sensing is achieved by mounting the IoT devices on the transport partners' vehicles or private partners' traffic signals. First, we have performed the micro-benchmarking of the designed IoT device. Next, the IoT devices are deployed at various places on campus and at traffic intersections. Based on the data collected from multiple places, we have performed the Particulate Matter factor correlation analyses. We have additionally observed that scalable sensing gives rise to various security concerns, e.g., IoT devices are vulnerable to malware attacks. IoT devices can also be compromised easily when default configurations are used. Further, in a complex system of air pollution sensing, different stakeholders participate. Each stakeholder has its own set of privacy and security requirements. One of the stakeholders, i.e., the transport partners, is sensitive about releasing their vehicles' locations and fleet size as this may reveal their business model to rival companies. The sensor data clients also want to hide their query locations.

When there is little or no trust among the different stakeholders in this complex ecosystem, data integrity has to be carefully reasoned about. In this thesis, we have presented a combination of *pre-deployment verification* and *post-deployment attestation* to provide data integrity guarantees to IoT devices running heavy-compute applications such as pollution monitoring. Pre-deployment verification ensures that the sensed data is sent to the appropriate servers of the deployment partners to avoid data privacy violations. It also ensures that our implemented software does not favor any party in a policy debate by verifying the non-interference property among different sensors. The non-interference property implies that based on the sensed value of one sensor, e.g., GPS, the code does not modify the sensed value of another sensor, e.g., PM.

This thesis has also proposed *PracAttest*, a post-deployment attestation framework that employs the Trusted Execution Environment architecture. In the prior works, we have found that the issue of regular runtime attestation of the deployed software, with negligible EdgeML performance degradation, is not resolved. PracAttest facilitates a better performance-vs-security trade-off in IoT devices running extremely compute-intensive EdgeML workloads. It has provided 50x-80x speedup over the state-of-the-art baseline in terms of mean attestation time, with negligible impact on application performance.

To provide privacy guarantees to different stakeholders, we have defined a real-life *privacy-vs-utility trade-off* problem for air pollution monitoring based on anecdotal discussions. Transport partners and clients both have their own privacy requirements. The transport partner wants to hide the fleet size and location, while the clients want to hide the query locations. The utility of reporting accurate pollution values and associated measurement errors is also necessary. The utility concerns are exactly converse of the privacy concerns: environmentalists may want to know the sample size and locations to decide the merit of the pollution value for their analyses, while the cab fleet owners want to keep the detailed information of the sensed samples to be private. To provide privacy-utility guarantees, we have used a combination of Gaussian Process Regression, Secure Multiparty Communication, and Differential Privacy. Using real taxi trajectories and pollution datasets of different cities, these trade-offs and computational overhead for our methodology are shown to be achievable. For a given source-destination pair, we have also built a sample end-to-end Android application that gives the least polluted route alternatives in a privacy-preserved manner.

## सार

सतत विकास के विभिन्न मुद्दे हैं। उनमें से वायु प्रदूषण सबसे महत्वपूर्ण है। दिल्ली में बहुत कम वायु गुणवत्ता निगरानी स्टेशन हैं लेकिन बहुत सारी विवादास्पद नीतिगत बहसों हैं। इसने हमें वायु प्रदूषण की निगरानी के लिए कम लागत वाला मापनीय संवेदन समाधान तैयार करने के लिए प्रेरित किया है। परिवहन भागीदारों के वाहनों (सार्वजनिक बसों, जैसे, डी.आई.एम.टी.एस या टैक्सी, जैसे, ओला) पर आई.ओ.टी उपकरणों को माउंट करके मापनीय संवेदन प्राप्त की जाती है। हमने आई.ओ.टी उपकरण की माइक्रोबेंचमार्किंग की। इसके बाद इसे परिसर और परिवहन चौराहों के विभिन्न स्थानों पर तैनात किया गया। इन स्थानों से एकत्र किए गए आंकड़ों के आधार पर, हमने पीएम कारक सहसंबंध विश्लेषण किया। हमने देखा है कि मापनीय संवेदन विभिन्न सुरक्षा और गोपनीयता चिंताओं को जन्म देती है।

इस शोध प्रबन्ध में, हमने प्रस्तुत किया है कि कैसे प्रदूषण निगरानी या यातायात नियंत्रण अनुप्रयोगों को चलाने वाले आई.ओ.टी उपकरणों को पूर्व-तैनाती सत्यापन और परिनियोजन के बाद सत्यापन का उपयोग करके सुरक्षित बनाया जा सकता है। पूर्व-तैनाती सत्यापन सुनिश्चित करता है कि नियोजित आँकड़े उचित गंतव्य यू.आर.एल पर जाता है ताकि तैनाती भागीदारों के लिए डेटा गोपनीयता उल्लंघन से बचा जा सके। हम सत्यापित करते हैं कि हमारा कार्यान्वित सॉफ्टवेयर नीतिगत बहस में किसी का पक्ष नहीं लेता है। पिछले शोध कार्यों में, हम पाते हैं कि नगण्य एजएमएल प्रदर्शन गिरावट के साथ तैनात सॉफ्टवेयर के नियमित कार्यावधि सत्यापन का मुद्दा अभी भी अनसुलझा है।

यह प्रबन्ध प्रैकएटेस्ट का प्रस्ताव करती है, जो एक परिनियोजन सत्यापन ढांचा है जो विश्वसनीय निष्पादन पर्यावरण वास्तुकला को नियोजित करता है। यह अत्यधिक गणना-गहन एजएमएल कार्यभार चलाने वाले आई.ओ.टी उपकरणों में एक बेहतर प्रदर्शन-बनाम-सुरक्षा की सुविधा प्रदान करता है। यह औसत सत्यापन समय के संदर्भ में आवेदन प्रदर्शन पर नगण्य प्रभाव के साथ अत्याधुनिक आधार रेखा पर 50x-80x गति वर्धन प्रदान करता है।

हमने एक अद्वितीय गोपनीयता-उपयोगिता दुविधा की पहचान और वर्णन भी की है जो तब उत्पन्न होता है जब ग्राहक वायु प्रदूषण मूल्य के लिए परिवहन भागीदारों के सर्वर से पूछताछ

करते हैं। परिवहन भागीदार गाड़ियों के समूह के आकार और स्थान को छिपाना चाहता है जबकि ग्राहक परिप्रश्न स्थानों को छिपाना चाहता है। हमने परिवहन भागीदारों और ग्राहकों दोनों को समाधान प्रदान करने के लिए गॉसियन प्रोसेस रिग्रेशन, सिक्वोर मल्टीपार्टी कम्युनिकेशन और डिफरेंशियल प्राइवैसी के संयोजन का उपयोग किया है। हमने एक छोर-से-छोर एंड्रॉइड एप्लिकेशन नमूने के तौर बनाई पर है जो कम से कम प्रदूषित मार्ग विकल्प को गोपनीयता संरक्षित तरीके से देता है।

# Contents

<b>Certificate</b>	<b>i</b>
<b>Acknowledgements</b>	<b>iii</b>
<b>Abstract</b>	<b>v</b>
<b>LIST OF TABLES</b>	<b>xvi</b>
<b>LIST OF FIGURES</b>	<b>xxi</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Scalable Sensing . . . . .	2
1.1.1 Types of Low-cost Sensors . . . . .	3
1.1.2 Mode of Sensing . . . . .	3
1.2 Key Challenges in Low-cost Sensing . . . . .	4
1.2.1 Microbenchmarking of Sensors . . . . .	4
1.2.2 Data Integrity . . . . .	4
1.2.3 Requirements of Key Stakeholders . . . . .	5
1.3 Contribution of the Thesis . . . . .	9

1.3.1	Framework Development and Microbenchmarking of Low-cost IoT Device for Air Quality Measurement with Factor Correlation Analysis . . .	9
1.3.2	Attestation of EdgeML Devices . . . . .	11
1.3.3	Privacy Issues in Urban Sensing . . . . .	11
1.4	Organization of the Thesis . . . . .	13
<b>2</b>	<b>LOW-COST PM MONITORING AND FACTOR CORRELATION</b>	<b>15</b>
2.1	Introduction . . . . .	15
2.2	Related Work . . . . .	18
2.3	Explored PM Related Policy Debates . . . . .	19
2.4	System Goals . . . . .	22
2.4.1	Scalable Measurements . . . . .	22
2.4.2	Incentives for Transport Partners . . . . .	22
2.4.3	Data Integrity and Privacy . . . . .	23
2.5	IoT Design . . . . .	24
2.5.1	Sensors Requirement . . . . .	24
2.5.2	PolIoT: IoT Software . . . . .	25
2.5.3	Hardware Platforms . . . . .	26
2.6	Performance Evaluation . . . . .	28
2.6.1	Micro-benchmarking . . . . .	29
2.6.2	Static Deployment . . . . .	33
2.6.3	Vehicular Deployment . . . . .	33
2.7	Factor Analysis for Particulate Matter (PM) Data . . . . .	35
2.7.1	Static Factor Analysis for PM <sub>2.5</sub> . . . . .	36

---

2.7.2	Dynamic Factor Analysis for PM 2.5 . . . . .	38
2.8	Conclusion and Future Work . . . . .	46
<b>3</b>	<b>PRE-DEPLOYMENT VERIFICATION</b>	<b>47</b>
3.1	Introduction . . . . .	47
3.2	Automatic Verification Tools Background . . . . .	48
3.3	Related Work . . . . .	49
3.4	Threat Model and Assumptions . . . . .	50
3.5	Privacy and Security Goals . . . . .	50
3.5.1	Data Privacy . . . . .	50
3.5.2	Data Integrity . . . . .	51
3.6	PolIoT Information Flow Policy . . . . .	52
3.6.1	Data Privacy . . . . .	52
3.6.2	Non-Interference . . . . .	53
3.7	Implementation Details . . . . .	53
3.7.1	Are Violations Correctly Caught? . . . . .	53
3.7.2	Are False Alarms Easy to Analyze? . . . . .	56
3.8	Conclusion . . . . .	58
<b>4</b>	<b>POST-DEPLOYMENT ATTESTATION</b>	<b>59</b>
4.1	Introduction . . . . .	59
4.2	Related Work . . . . .	62
4.3	System and Threat Model . . . . .	64
4.3.1	Threat Model . . . . .	64

4.3.2	System Architecture . . . . .	64
4.4	PracAttest Design . . . . .	66
4.4.1	Selecting Kernel Segment . . . . .	68
4.4.2	Determining Inter-Attestation Time . . . . .	69
4.5	Verified EdgeML Benchmarks . . . . .	72
4.5.1	Benchmark Applications . . . . .	72
4.5.2	Benchmark Verification . . . . .	75
4.6	Evaluation . . . . .	76
4.6.1	Experimental Setup . . . . .	77
4.6.2	Evaluation Metrics . . . . .	77
4.6.3	Number of Kernel Segments To Be Attested . . . . .	78
4.6.4	Inter-Attestation Time Distribution . . . . .	79
4.6.5	PracAttest Performance-Security Trade-off . . . . .	80
4.7	Conclusion and Future Work . . . . .	83
<b>5</b>	<b>PRIVACY IN URBAN SENSING</b>	<b>85</b>
5.1	Introduction . . . . .	85
5.2	Background . . . . .	88
5.2.1	Gaussian Process Regression(GPR) . . . . .	88
5.2.2	Root Mean Squared Error (RMSE) . . . . .	89
5.2.3	Differential Privacy (DP) . . . . .	89
5.2.4	Secure Multiparty Computation . . . . .	90
5.3	Related work . . . . .	91
5.4	Datasets . . . . .	92

---

5.5	System Architecture . . . . .	93
5.5.1	Query Granularity . . . . .	94
5.5.2	Query Types and Output . . . . .	95
5.5.3	Threat Model and Privacy Policy . . . . .	96
5.6	Interpolation with Gaussian Process Regression . . . . .	97
5.6.1	Processing of the Data . . . . .	98
5.6.2	Accuracy of Posterior Mean $\mu_p$ . . . . .	99
5.6.3	Computational Complexity of GPR . . . . .	100
5.6.4	GPR Output . . . . .	101
5.6.5	Privacy Guarantees with GPR . . . . .	102
5.6.6	GPR Output Leaks Information . . . . .	104
5.7	Differentially Private Pollution Maps . . . . .	104
5.7.1	Sensitivity Calculation for $\sigma_p^2$ . . . . .	105
5.7.2	Computation Time for DP . . . . .	106
5.7.3	DP Pollution Maps Output . . . . .	106
5.7.4	Balancing Client Utility vs. Fleet Privacy . . . . .	107
5.7.5	Further Fleet Privacy Concerns with DP . . . . .	108
5.8	Query Response System Using Secure 2PC . . . . .	109
5.8.1	Prac2PC- Secure 2PC Protocol . . . . .	109
5.8.2	Circuit Components . . . . .	113
5.8.3	Query Function with Error Propagation . . . . .	114
5.8.4	Adding Differential Privacy . . . . .	117
5.9	End-to-end Security Analysis . . . . .	117

5.10	Prac2PC Implementation . . . . .	119
5.10.1	Prac2PC Variants . . . . .	119
5.10.2	Experimental Setup For Evaluations . . . . .	120
5.11	Prac2PC Evaluation . . . . .	121
5.11.1	Realistic $v$ Sizes . . . . .	121
5.11.2	Prac2PC Runtimes and CPU Utilization . . . . .	122
5.11.3	Prac2PC Bandwidth . . . . .	124
5.11.4	Prac2PC-Malicious . . . . .	126
5.11.5	Server Privacy vs. Client Utility . . . . .	127
5.12	End-to-End System with GPR and Prac2PC . . . . .	128
5.13	Discussion on Multithreading . . . . .	130
5.14	Conclusion and Future Work . . . . .	131
<b>6</b>	<b>FUTURE WORK AND CONCLUSION</b>	<b>133</b>
6.1	Future Work . . . . .	133
6.2	Conclusion . . . . .	135
	<b>Bibliography</b>	<b>137</b>
	<b>List of Publications</b>	<b>157</b>
	<b>Biography</b>	<b>159</b>

# List of Tables

2.1	Related work on air pollution sensing . . . . .	19
2.2	Driving anomaly detection . . . . .	20
2.3	Sensors and their uses . . . . .	25
2.4	Software components . . . . .	25
2.5	Concurrent threads running in a loop . . . . .	26
2.6	Hardware cost . . . . .	27
2.7	Resource usage and heating . . . . .	32
3.1	PollIoT’s IFC policy for non-interference . . . . .	52
3.2	System and tool configurations . . . . .	54
3.3	Results demonstrating that the number of false positives start decreasing once we identify the cause. . . . .	57
4.1	Qualitative comparison of PracAttest with the prior works. . . . .	63
4.2	Notation utilized for the parameters in PracAttest. . . . .	68
4.3	Concurrent threads running in PollIoT. . . . .	72
4.4	Mean kernel attestation and inference time comparison. . . . .	80
5.1	Summary of datasets used to evaluate different techniques . . . . .	93

---

5.2	Prac2PC supported queries, with client inputs and outputs. Propagated error discussed in Section 5.8.3 . . . . .	95
5.3	Interpolation techniques comparison . . . . .	97
5.4	Query function and error propagation formulae, implemented in the Garbled Circuit where $S(y_i, \theta) = \frac{1}{1 + \exp(-(y_i - \theta))}$ . . . . .	114
5.5	Client-Server configuration . . . . .	121
5.6	Latency and CPU utilization for Android as client with ping latency of 20ms ~ 80ms . . . . .	123

# List of Figures

1.1	Air quality map of the world. Parts of the world colored yellow, orange, red, and purple indicate the breach of the air quality limits set by WHO. According to the WHO, around 94% of the deaths caused by air pollution are in low- and middle-income nations. Regions of Africa, Eastern Europe, India, China, and the Middle East, colored darker red, are most affected by pollution. <i>Source:WHO</i>	1
1.2	Delhi with fixed air quality monitoring stations . . . . .	3
1.3	Overall system architecture . . . . .	8
1.4	Major contribution done during the PhD. . . . .	8
2.1	Hardware components . . . . .	27
2.2	IoT unit mounted on different locations . . . . .	28
2.3	Hardware platform second prototype showing the sensors, micro-controller, inside ABS plastic boxes. . . . .	29
2.4	Hardware platform second prototype multiple units. These were deployed in university campus, at traffic intersections etc. . . . .	30
2.5	IoT device's performance benchmark . . . . .	30
2.6	Low-cost sensor's PM 2.5 values on the left vs. a co-located TSI DustTrak's PM 2.5 values on the right, on a sample day. While their costs are 30 USD and 10K USD respectively, i.e. an order of magnitude different, their measured PM values are still comparable. . . . .	32
2.7	PM 2.5 sensed by vehicle-mounted devcie in the year 2019 . . . . .	34

2.8	IMU data sample . . . . .	35
2.9	PM 2.5 measured by varying the speed of vehicle . . . . .	36
2.10	Correlation plots between static factors like %builtup, %greencover and %residential with PM 2.5 for sample day 134 . . . . .	38
2.11	Average PM 2.5, as recorded by IoT mounted units in campus and traffic intersections . . . . .	39
2.12	Sample sensor locations in university campus . . . . .	40
2.13	PM 2.5 count at traffic intersection . . . . .	40
2.14	Sensor6 PM count in summer . . . . .	41
2.15	Vehicle count at traffic intersection . . . . .	41
2.16	Negative correlation between temperature and PM . . . . .	42
2.17	Meteorological effects on PM values . . . . .	43
2.18	Combined effects of traffic and meteorological phenomenon on PM values . . . . .	44
3.1	Lattice for PolIoT non-interference requirements (any information flow between sensor nodes is considered illegal). . . . .	53
3.2	Simplified program dependence graph corresponding to Listing 3.2. . . . .	55
4.1	Comprehensive system architecture for securing IoT devices. The one-time pre-deployment verification of security requirements is conducted based on the policies specified by the IoT device developers and users (e.g., the EdgeML data servers and clients). The runtime attestation of the deployed software (running in the normal world) is conducted with the help of the hardware root of trust (in the secure world). The attacker aims to compromise the software running in the normal world. . . . .	64
4.2	Continuous attestation hampers application in the Conventional Software Attestation (CSA) scheme. . . . .	66

4.3	Flexible coexistence of attestation and application in PracAttest (the spaces represent the CPU idle time, the red lines represent the application execution time, the purple lines represent the kernel attestation time, and the green lines represent the CPU usage sampling time) . . . . .	71
4.4	CPU usage profile for the EdgeML benchmarks. . . . .	74
4.5	Ratio of segments selected for attestation and total segments ( $n = 2130$ ) vs. $P_f$ for a non-roving malware. . . . .	78
4.6	Ratio of segments selected for attestation and total segments ( $n = 2130$ ) vs. $P_f$ for a roving malware. . . . .	79
4.7	CDF plots of inter-attestation time in different EdgeML benchmarks. . . . .	81
4.8	Shadow-Box inter-attestation times. Inter-attestation time selected for attesting kernel entries is constant i.e. the monitored CPU usage always remain high. . .	82
4.9	Mean attestation time for varying ratio of random segments and total segments ( $n = 2130$ ) required for hashing to achieve a fixed $P_f (\approx 0)$ . . . . .	83
5.1	Coverage with 3 routes where we instrument buses with air pollution sensors in Delhi. Government deployed static pollution sensors are shown with landmark icons. . . . .	86
5.2	System architecture preserving privacy for server and client with different privacy, utility, and overhead. . . . .	94
5.3	City $\mathcal{A}$ divided into squares with blue squares representing the client's area of interest and red/green rectangles representing the client's preferred obfuscation levels. . . . .	95
5.4	Gaussian Process Regression output with and without standardization . . . . .	99
5.5	RMSE of Posterior mean ( $\mu_p$ ) vs. Different Kernels . . . . .	100
5.6	(a) Time taken for training different number of sample locations sensed by the 24 cabs in 24 hours for 7 days. (b) Prediction Time vs Number of grid cells . .	101
5.7	Pollution Map for Beijing using GPR . . . . .	102

5.8	Trajectory shows every vehicle locations (left side), Interpolation subsumes individual vehicle location in a grid cell (right side) . . . . .	102
5.9	Interpolation output for the case where trajectory can be seen in the posterior variance contour plot . . . . .	103
5.10	DP time vs Number of grid cells . . . . .	106
5.11	DP plots corresponding to different $\epsilon$ for the case where trajectory can be seen in the posterior variance contour plot . . . . .	107
5.12	Utility-vs-Privacy for different cities in terms of CDF of RMSE for different hours. . . . .	108
5.13	Circuit details of Prac2PC . . . . .	110
5.14	Smartly crafted queries where subsequent queries overlap by a single grid square (marked in red). . . . .	111
5.15	Prac2PC-Malicious workflow. Red boxes represent the steps that are performed by both client and server independently. Blue boxes represent computation at only the server-side, and blue arrows represent data coming from the server. Similarly green boxes and arrows are for Client (subscript $s$ denotes server share and subscript $c$ denotes client share, $v, \mu, \sigma^2$ are inputs as discussed in 5.8). . .	120
5.16	(a) Trip length vs. $v$ size for 7500 trips. (b)-(d) Runtimes for different query types and Prac2PC versions . . . . .	122
5.17	Average CPU Usage for different query . . . . .	124
5.18	Data transfer between server and client for different query types and Prac2PC versions. Here, the number of bytes server received in Prac2PC-GC is negligible enough to be visible in plots. . . . .	125
5.19	Query latency for Prac2PC-Malicious . . . . .	126
5.20	Privacy-utility trade-off . . . . .	127
5.21	PM sensors, raw locations and values measured using static campus deployment	128
5.22	Interpolated map for university campus . . . . .	128
5.23	Privacy-aware Pollution Route App . . . . .	129

---

5.24 Energy profile monitored using Android Studio for range query with  $v = 100$ .  
Both network and CPU energy usage profiles are low. . . . . 130