PRIVACY, INTEGRITY AND PERFORMANCE OF EDGE DEVICES FOR SUSTAINABILITY

ISMI ABIDI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
October 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 Philosphy** 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. *Alhamdullilah!!*

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 है। उनमें से वायु प्रदूषण सबसे महत्वपूर्ण है। दिल्ली में बहुत कम वायु गुणवत्ता निगरानी स्टेशन हैं लेकिन बहुत सारी विवादास्पद नीतिगत बहसें 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 सॉफ़्टवेयर 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, सिक्योर मल्टीपार्टी कम्युनिकेशन और डिफरेंशियल प्राइवेसी 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

List of Tables

List of Figures