



Sensor Data Attestation Based on Contractual Policies

Aditya Krishnan, Dr. Sharad Mehrotra, Dr. Roberto Yuspeir, Dr. Nisha Panwar

¹Santa Clara University

²Donald Bren School of Information and Computer Sciences University of California, Irvine

NSF REU IoT-SITY Summer Research Program



Introduction

This project deals with creating a structure for attestation of sensor data in infrastructures where multiple parts of the data capture is taken into consideration. The ideas that represent the process of attestation are related to determining how policies for data capture are to be created and tabulated, how user's within the infrastructure are notified of the active policies, how logs are stored and sealed for later infrastructure travel, and with regards to the algorithm for attestation on the logs and implementation of this algorithm.

Procedure

Policy Language and Creation

Need to create a generic policy language to use as a structure for data capture policies that are to be created. Creation is done through TIPPERS, a smart building application suite that monitors Donald Bren Hall.

Informed Consent

It is important to notify users who enter the infrastructure about active policies and save their consent.

Logging and Log Sealing

Logs made by infrastructure devices and user consent are to be saved with all necessary information in a log managing database in TIPPERS.

After logs are created, logs must be sealed using a hash chain for attestation.

Procedure

Attestation

Attestation is a proof measure for obtaining evidence with regards to data capture policies to show that the infrastructure did as it said it would to the user. This keeps the infrastructure and user in check.

Attestation involves creation of an algorithm that will provide users with all necessary information for valid evidence and proofs without tampering of the logs being allowed.

Implementation

Informed Consent is the main aspect worked on during the last 8 weeks. This involved originally using email to send users links regarding the different possible responses that a user can commit to with regards to the policies on data capture. The final method of implementation involved saving policy information and log information in TIPPERS through database managers that are updated through IoT. This is an Android application that is linked to the database through an Informed Consent resource. The user can simply toggle a switch that enables them to agree or not agree to the policy at hand.

Attestation with regards to informed consent enables users to attest what consent they gave, whether they opted in or opted out. Also it enables the user to take note of policy information.

TIPPERS

TIPPERS is an application suite live in Donald Bren Hall (DBH) that monitors humidity, temperature, and sensor health settings in the building. It works to make DBH a smart building by monitoring and providing statistics to users who are registered on the portal.



Donald Bren School of Information and Computer Sciences

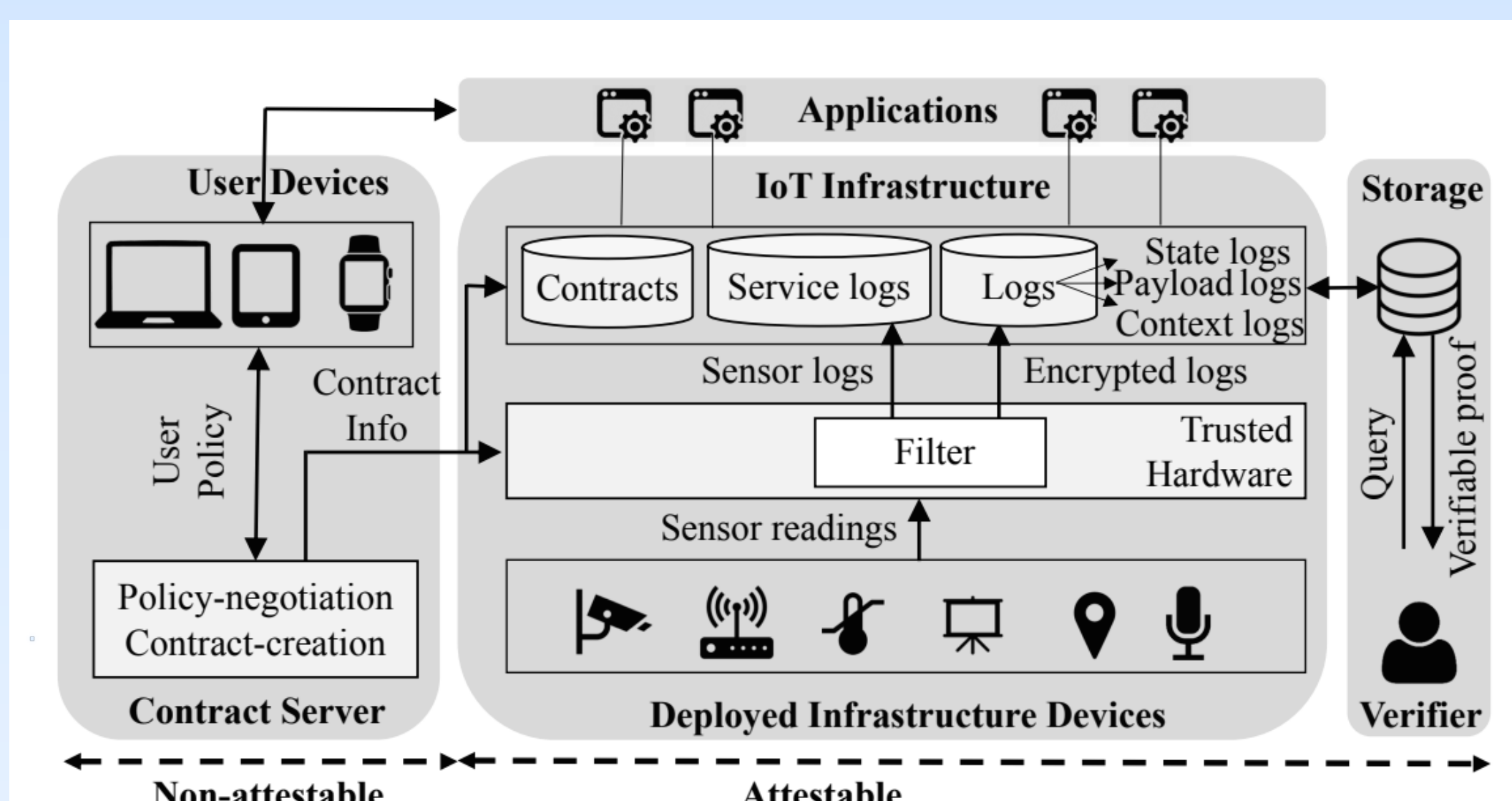


Figure 1: System model

ACKNOWLEDGEMENTS: I would like to thank Professor Sharad Mehrotra for hosting me through the IoT-SITY Program and all the other students in his lab who aided me in completing this project. I would also like to thank Professor Sharnnia Artis and Professor Nalini Venkatasubramanian for allowing me to participate, as well as Martha Osegueda for being a mentor throughout the duration of this program. I would also like to thank NSF for sponsoring and funding the REU program.

Conclusion

Overall, research has involved learning how to create databases and tables in MySQL, re-enforcing my knowledge and use of Java, and learning about new concepts that are important to how privacy is dealt with in a larger setting.

Future Work

Implementing a coverage and inverse coverage aspect to TIPPERS that allows for a mapping of regions that are shared in coverage between cameras, wifi access points, and other sensors in the building. Also, this would include improving the definition of opting out with respect to attestation. No can be made to include more than simply leaving the premises being monitored. This is dependent on an inclusion of negotiation in policy definitions.

References

- . 2018. IoT Notary for Retroactive Consents, Compliance and Audits. In Proceedings of . ACM, New York, NY, USA, 13 pages. <https://doi.org/10.1145/nnnnnnnn.nnnnnnnn>
- Henze, Martin, et al. "Cppl." *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society - WPES'16*, 24 Oct. 2016, doi:10.1145/2994620.2994627.

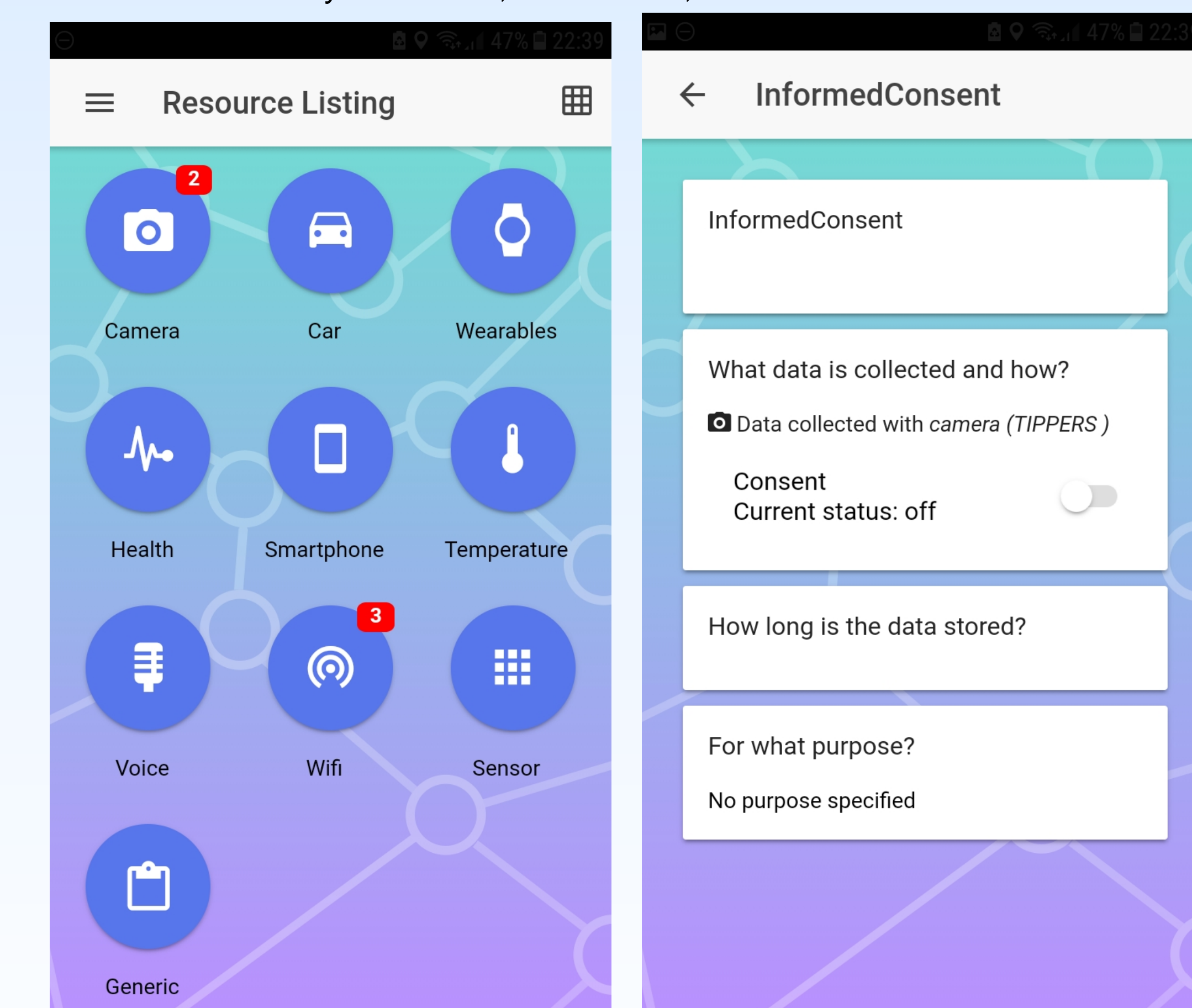


Figure 2 & 3: The IoT Android Application Layout