Privacy in the Smart City —Applications, Technologies, Challenges, and Solutions

秦睿阳

Content

- 1.Introduction
- 2.Taxonomies（分类）
- 3. Building Blocks for Privacy Protection
- 4. Privacy Challenges & Solutions
- 5.Conclusion

Introduction

- The number of smart city applications is large .
- The effectiveness of these and other smart city applications heavily relies on data collection.

Unfortunately, this is also the reason why smart cities pose a major threat to the privacy of citizens .

Introduction

Our main contributions are:

- A、taxonomies
- B、We present an overview of building blocks for privacy protections
- C、For each enabling technology, we identify privacy threats and describe possible solution
- D、We review examples of smart city applications that have already been realized in cities around the world and analyze which privacy protections have been deployed.
- E、We discuss research directions that could contribute to privacy protection in smart cities.

Taxonomies

1、 *Smart City Applications*

- A、*Smart Mobility*
- *B*、*Smart Utilities*
- C、*Smart Buildings*
- D、*Smart Environment*
- *E*、*Smart Public Services*
- *F*、*Smart Governance*
- *G*、*Smart Economy*
- *H*、*Smart Health Care*
- I、*Smart Citizens*

Taxonomies

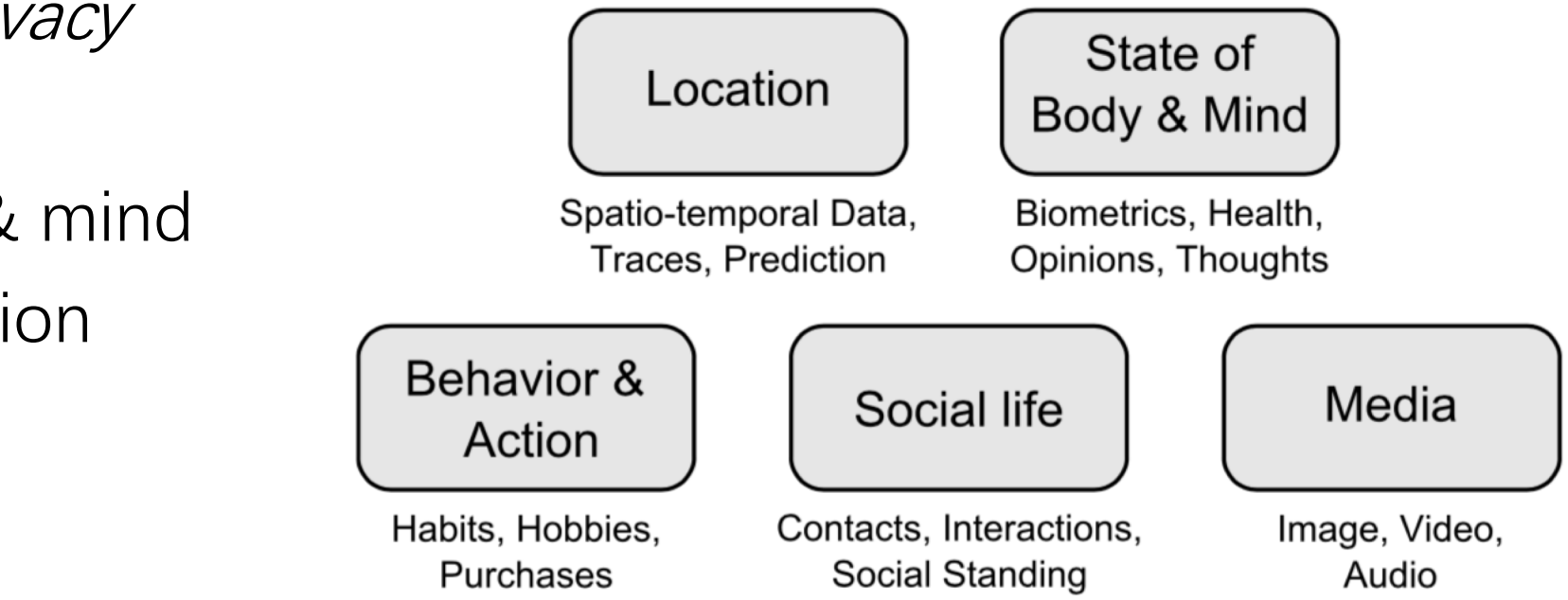
2、 *Enabling Technologies*

- A、Ubiquitous Connectivity
- B、Smart Cards
- C、Sensor Networks
- D、Wearable Devices
- E、the Internet of Things
- F、Intelligent Vehicles
- G、Autonomous Systems
- H、Cloud Computing
- I、Open Data

Taxonomies

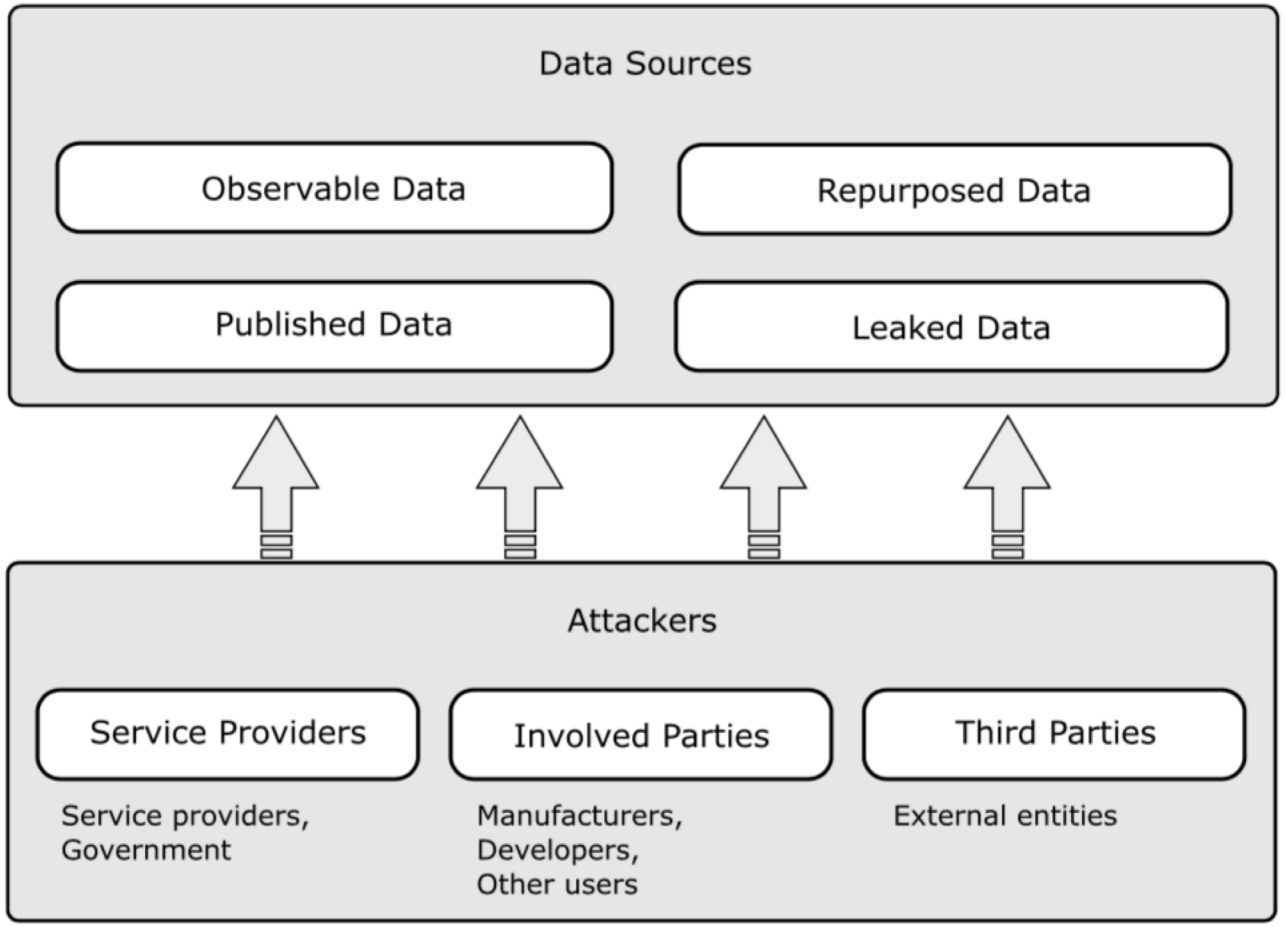
3、*Five Types of Privacy*

- A、location
- B、state of body & mind
- C、behavior & action
- D、social life
- E、media



Taxonomies

4、Attackers and Data Sources



Building Blocks for Privacy Protection

1、*Process-Oriented Privacy Protection*

- A、*Privacy by Design*
- B、*Privacy Requirements Engineering*
- C、*Testing and Verification*
- *D*、*Transparency*
- E、*Consent and Control*
- *F*、*Auditing and Accountability*

Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

- *A、Data Minimization*
- B、*Data Anonymization*
- *C、Differential Privacy*
- *D、Encryption*
- *E、Homomorphic Encryption*
- F、*Zero-Knowledge Proofs*
- G、*Secret Sharing*
- H、*Anonymous/Pseudonymous Digital Credentials*
- I、*Secure Multi-Party Computation*
- *J、 Private Information Retrieval*

Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

A、Data Minimization

Sensors of modern smart systems naturally gather more sensor data than required for the envisioned task.So we need to process the raw data.

Example:

Cameras for specific tasks such as face recognition or traffic surveillance also record unrelated information

Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

B、*Data Anonymization*

Remove the identifying information, and ensure that all equivalence classes have at least *k* rows.

邮编	年龄	疾病
47677	29	心脏病
47602	22	心脏病
47678	27	心脏病
47905	43	流感
泛化之后		
476**	2*	心脏病
476**	2*	心脏病
476**	2*	心脏病
479**	4*	流感

Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

C、Differential Privacy

Any disclosure is equally likely regardless of whether or not an item is in the database .

id	姓名	年龄	…	是否有癌症
1	某某1	47		否
2	某某2	43		是
	…			
7	张三	45		是

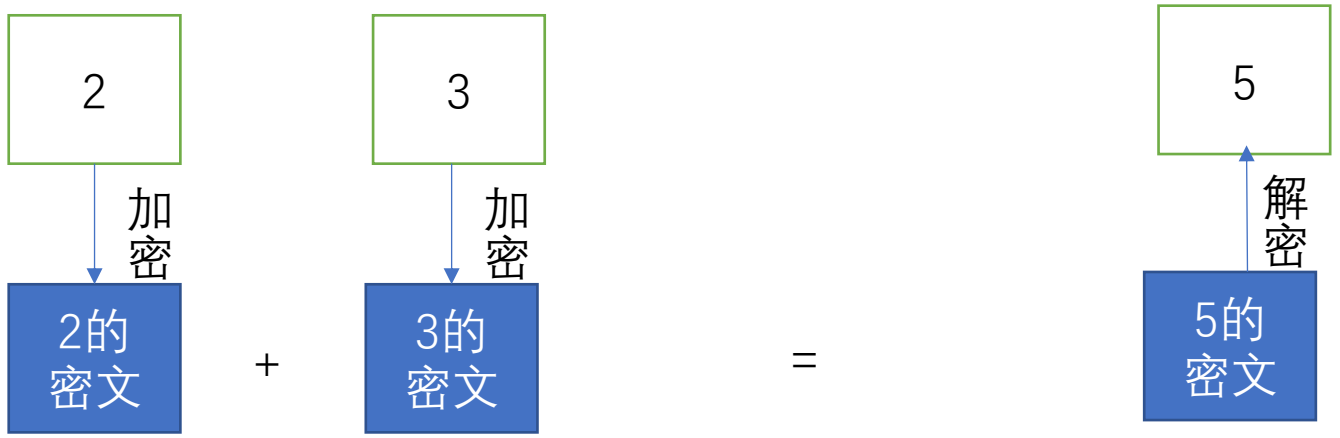
Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

D、Encryption

E、Homomorphic Encryption

Homomorphic encryption (HE) is a cryptographic method that allows computations on encrypted data and thus protects confidentiality during data processing.



Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

F、*Zero-Knowledge Proofs*

Zero-knowledge proofs are a cryptographic method that allows one party (the prover) to prove their knowledge of some fact to another party (the verifier), without revealing the fact or any other information.

Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

G、*Secret Sharing*

Secret sharing is a method that allows to distribute secret information among several participants.

In smart cities, secret sharing can be used in solutions for data aggregation, for distributed data storage.

Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

H、*Anonymous/Pseudonymous Digital Credentials*

Anonymous digital credentials provide a privacy-preserving way for individuals to prove facts about them without revealing their identity.

Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

I、*Secure Multi-Party Computation*

Secure multi-party computation is a cryptographic method that allows two or more parties to jointly compute the value of a public function with- out revealing the parties' private inputs, and without relying on a trusted third party.

Building Blocks for Privacy Protection

2、Data-Oriented Privacy Protection

J、 Private Information Retrieval

Private information retrieval allows clients to query database servers without revealing the query or the query results to the server.

Building Blocks for Privacy Protection

3、*No Privacy Without Security*

- A、*System security and access control*
- *B*、*Protocol and network security*
- *C*、*Information leakage*

Privacy Challenges & Solutions

A、 *Ubiquitous Connectivity*

(1) Privacy for the Communication Channel：

Challenge： mobile Internet providers can track their users via cell tower and hot spot locations

Solution： SSL/TLS

(2) *Privacy for Metadata：*

Challenge： metadata (who communicates with whom, when, and how long) needs to be protected

Solution： Use anonymous communication

(3) *Fingerprinting ：*

Challenge： Even when public Internet is used anonymously, fingerprinting techniques using static MAC addresses

Solution： change device identifiers frequently, randomize browser fingerprints, and insert cover traffic

(4) *Privacy for Mobile Devices ：*

Challenge： Modern mobile devices are equipped with a multitude of sensors. In addition, these devices consist of various components developed by different parties with different goals and incentives.

Solution：Use minimal permissions for mobile apps, avoid use of third-party libraries

Privacy Challenges & Solutions

B、 *Smart Cards*

Challenge：

The main privacy issue in smart cards is the logging of transactions.

Solutions：

（1）Separation of authentication and service

（2）Data minimization：do not store identifiers of smart cards

Privacy Challenges & Solutions

C、*Open Data*

Challenge：

Simply removing all personally identifying information is not a sufficient protection against de-anonymization.

Solutions：

（1） *Aggregation：release noisy aggregates of data（differential privacy）*

（2） *Obfuscation：Release only data that satisfy k-anonymity, l-diversity, m-invariance, or t-closeness*

Privacy Challenges & Solutions

D、*Sensor Networks*

Challenge：

Unlike environmental sensors (e.g., in forests or the ocean), sensors in the smart city monitor the very space citizens live in and may thus collect sensitive data.

Solutions：

（1）*Data Minimization：Isolate sensors from other systems, optimize placement to collect no PII. Extract relevant features on sensor, discard raw data.*

（2）*Aggregation：Aggregate sensor readings from multiple participants privately. (Homomorphic Encryption)*

(3) Location Cloaking：Data Anonymization

*(4) Separation of knowledge：*Splitting knowledge between different entities can reduce the risk of privacy violations.

Privacy Challenges & Solutions

E、*Wearable Devices*

Challenge：

The main privacy threats for wearable devices come from wireless eavesdropping, protocol design and software flaws, and side channel attacks.

Solutions：

(1)Reduce time and location granularity on device. Extract relevant features on device, discard raw data.(*Data Minimization)*

(2) Avoid storing encryption keys on device.

(3)Use secure distributed data storage. (secret share)

Privacy Challenges & Solutions

F、*Internet of Things*

Challenge：

The Internet of Things (IoT) enhances existing appliances with sensing and communication capabilities to collect data and enable applications. This allows service providers and involved parties to learn sensitive information about the people living in the monitored space.

Solutions：

（1） *Data Minimization*

*（2） Anonymization and Aggregation(*homomorphic encryption, secret sharing)

（3） Obfuscation

Privacy Challenges & Solutions

G、 *Autonomous Systems*

Challenge：

Autonomous systems, such as robots and drones, rely on various sensors, can give manufacturers and operators of autonomous systems access to sensitive data about the individuals the robot or drone comes into contact with.

Privacy for mobility services.（交通服务）

Solutions：

（1） *Data minimization*

（2） anonymous payment and authentication

Privacy Challenges & Solutions

H、 *Intelligent Vehicles*

Vehicles periodically broadcast their status, because these broadcasts are unencrypted, everyone in transmission range can link vehicles to locations and track their paths.

（1）Use short-lived pseudonyms for car-to-car communication.

（2）Eliminate mapping between short-term and long term identifiers.

（3）Process data for toll pricing on device, discard raw data.

Privacy Challenges & Solutions

I、 *Cloud Computing*

Cloud providers are used as part of public-private partner- ships to outsource storage and/or processing of arbitrary smart city data and services. This makes it necessary to consider privacy in the context of cloud computing in addition to the considerations for the underlying data or service.

(1) Hide access patterns to remote files and remote databases.

(2) Use attribute-based encryption for access control

(3) Privately process data at third parties(*Homomorphic Encryption*)

(4) *Anonymous/Pseudonymous Digital Credentials*

(5) Secure Multi-Party Computation

Conclusion

To break down the complexity of the smart city, we introduced taxonomies for application areas, enabling technologies, potential attackers, data sources for attacks, and different types of citizens' privacy.

These taxonomies allowed us to present a holistic analysis of privacy threats and possible solutions.

In summary, I hope that this systematic review of privacy in smart cities will support comprehensive privacy solutions for smart cities.

Solutions

PET	Technology	Privacy-Preserving Solution
Data Minimization	Ubiquitous Connectivity	Use minimal permissions for mobile apps, avoid use of third-party libraries [64]
	Smart Cards	Do not store identifiers of smart cards [203]
	(Participatory) Sensor Networks	Isolate sensors from other systems, optimize placement to collect no PII [13] Extract relevant features on sensor, discard raw data [204] Separate entities that ask for and receive sensor readings [40]
	Wearable Devices	Reduce time and location granularity on device [205], [206] Extract relevant features on device, discard raw data [78]
	Internet of Things	Process data for smart metering on device, discard raw data [47], [149]
	Intelligent Vehicles	Process data for toll pricing on device, discard raw data [150] Require cooperation of multiple entities to de-anonymize vehicles [207]
Data Anonymization	Ubiquitous Connectivity	Change device identifiers frequently to prevent fingerprinting [194], randomize browser fingerprints [195], insert cover traffic [196]
	Open Data	Release only data that satisfy k-anonymity[126], l-diversity [128], m-invariance[129], or t-closeness [130]
	(Participatory) Sensor Networks	Ensure k-anonymity of sensor readings [155] Ensure spatio-temporal readings cover at least k individuals [73], [208], [40] Use l-diversity [128] or hierarchical map quantization [209] to prevent location semantics attacks against k-anonymity
	Internet of Things	Cluster IoT data streams and only release clusters with at least k members [210]
Differential Privacy	Open Data	Release noisy aggregates of data [211], e.g., public transport data [212]
	(Participatory) Sensor Networks	Obfuscate locations with planar Laplace noise [135], [213]
	Internet of Things	Apply noise to meter readings [134]
Encryption	Ubiquitous Connectivity	Ensure correct usage of SSL/TLS with static analysis [184] Ensure correct usage of SSL/TLS with dynamically linked libraries [185] Secure public WiFi with WPA2 [65] Use anonymous communication to protect metadata [186], e.g. Tor [187]
	Wearable Devices	Avoid storing encryption keys on device [214] Use cryptographically enforced role-based access control [215]
	Internet of Things	Use identity-based encryption for private service discovery [137]
	Cloud Computing	Use attribute-based encryption for access control [139], [140]
Homomorphic Encryption	(Participatory) Sensor Networks	Aggregate sensor readings from multiple participants privately [216]
	Internet of Things	Aggregate data over multiple participants [79], e.g. energy consumption [217]
	Cloud Computing	Privately process data at third parties [143]
Zero-Knowledge Proofs	Internet of Things	Enforce honesty of device for local processing, e.g., for smart meters [47], [149]
	Intelligent Vehicles	Enforce honesty of vehicle for local processing, e.g. for electronic tolling [150]
Secret Sharing	Open Data	Use privacy-preserving data aggregation [218]
	(Participatory) Sensor Networks	Enforce k-anonymity of sensor readings cryptographically [155] Compute statistics over sensor readings from multiple participants privately [152]
	Internet of Things	Aggregate data over multiple participants privately [153], [217]
	Wearable Devices	Use secure distributed data storage [154]
Anonymous/Pseudonymous Credentials	Smart Cards	Authenticate users without identifying them [219], [159]
	Intelligent Vehicles	Use short-lived pseudonyms for car-to-car communication [160], [220], [221] Preserve backwards-privacy when revoking pseudonyms [222], [89] Eliminate mapping between short-term and long-term identifiers [157]
	Cloud Computing	Authenticate users based on attributes instead of identities [19]
Secure Multi-Party Computation	Cloud Computing	Process data with private inputs [223], e.g. genomic tests [164] Perform privacy-preserving data mining over distributed datasets [224]