.

ASRA:Emergency Service Provider In Smart Cities

1. Miss.Dusane Shital M., *Information Technology, PREC Loni, Maharashtra, India*
2. Miss.Ahire Rakhi M, *Information Technology, PREC Loni, Maharashtra, India*
3. Miss.Pawar Ashwini , *Information Technology, PREC Loni, Maharashtra, India*
4. Mr.Dongare Abhijit K, *Information Technology, PREC Loni, Maharashtra, India*

ABSTRACT

Smart cities accumulate and process large amount of data streams which raise security and privacy concerns at individual and community levels. Sizeable attempts have made to ensure security and privacy of inhabitants' data. However, security and privacy issues of smart cities are not confined to inhabitants only; service provider and local government have their own reservations – service provider trust, reliability of the sensed data, and data ownership, to name a few. In this research work we identified a comprehensive list of stakeholders and model their involvement in smart cities by using Onion Model approach. Based on the stakeholder model we presented a security and privacy framework for secure and privacy-aware service provisioning in smart cities.

Keyword: *smart city, emergency response, privacy, security*

---

1. INTRODUCTION

With the emergence of smart cities and new technologies e.g. Internet of Things (IoT) such as RFIDs, environmental sensors, actuators smart phones, wearable sensors, cloud computing and their applications in a city environment provide the opportunity to collect and effectively use large scale city data for information awareness and decision making . Data from these devices and/or new sources can be integrated with existing city data that is stored by various departments and local agencies and be analysed for application specific information and knowledge generation. Such processing and storage of large scale data can be performed in a cloud environment to satisfy quality of service requirements e.g. response time of end user queries by provisioning of cloud based virtually unlimited computational and storage facilities. However, with these opportunities there exist new threats to user and/or device privacy and confidentiality of data when communicated between two or more devices and/or users, and establishing trust on services and information. In addition, inherent cloud security issues e.g. storage at Remote data centres, physical access etc. can contribute further in dealing with smart cities data security issues. Managing such data from a smart city perspective require proper security and privacy measures which can help in establishing trust and adopting smart solutions in a city environment by various stakeholders including citizens. State of the art literature review indicates that smart city solutions e.g. SMARTI, IoT-A etc.

Require a comprehensive approach in dealing with smart city data security, user privacy and trust issues. A few attempts have been made to identify security and privacy concerns of future cities.

2. PROBLEM STATEMENT

The Problem is to determine the proof of concept for a context-aware emergency response system in a smart city

3. RELATED WORK

A cloud based solution for security and privacy management in smart cities is discussed .Various stakeholders are identified and a framework for end-to-end security/privacy features for trustable data acquisition, dissemination and service provision is developed. A trusted cells approach is presented in where the advent of secure hardware in personal IT devices motivates provisioning of data security at the edges of the internet via personal data servers running on smart phones set-top boxes, secure portable tokens etc. A five dimensional model of citizens' privacy in smart cities is presented. These are: identity privacy, query privacy, location privacy, footprint privacy and owner privacy. The authors show how existing privacy enhancing technologies can be used to preserve citizens'

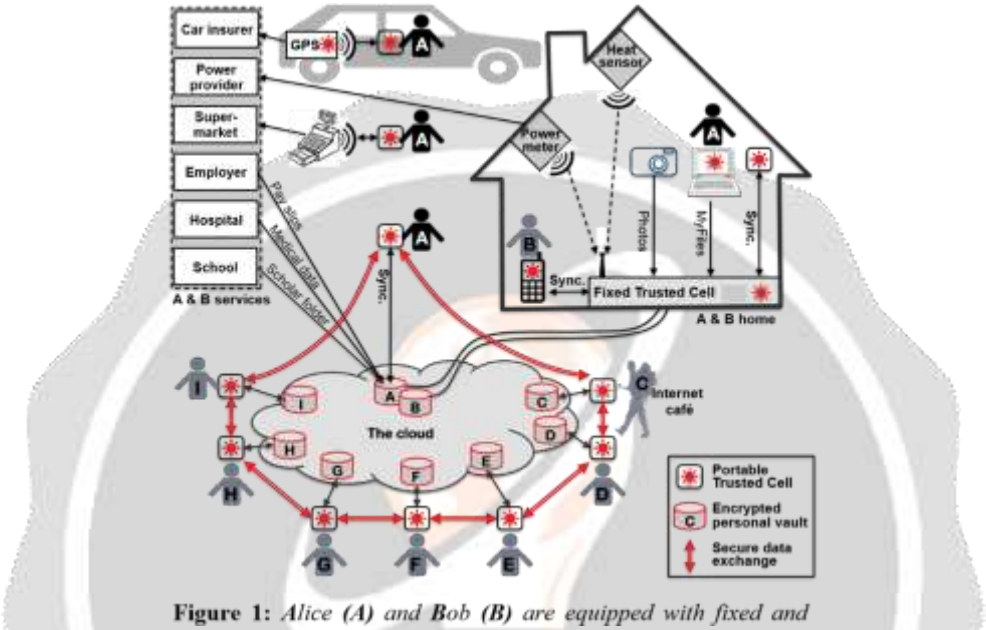

Figure 1: *Alice (A) and Bob (B) are equipped with fixed and*

Fig.1 Stop Word Process

4. SYSTEM ARCHITECTURE

4.1 **Smart building**

Equipped with a hybrid indoor positioning and tracking, motion detection and sensing system. A server on the LAN, the aggregation module, fuses information collected from various sources on the wireless network. It runs a navigation engine which converts measurements into location information. The collected information, comprising of the building occupancy distribution, individual identities of the occupants, their locations and movements as well as the ambient conditions is sent over a secure connection to a secure external location (in our architecture, this is the community cloud). The organization that manages the smart building is a part of the community cloud. In the event of an emergency, an emergency alert is sent to the community cloud.

4.2 **Management Server Database (MSB)**

It is used for the privacy and security concern for our database which we will stored in MSB.It provide the access control to the different databases present in our system. Its provide the application information to emergency response through the management server database. Provide approach to periodic updates on building occupancy to the emergency service provider with Sharp granularity.

4.3 **Emergency service provider**

Is a member of the management server database and has access to sharp-grained data during normal operations in order to supply out routine monitoring movement. In the event of an emergency, the ESP will identify the specific first responders indicate to handle the response operation and will alert the MSB with this information, transfer in an 'employee dispatch report'. These specific first responders will then gain approach to the required fine-grained data from the management server database.

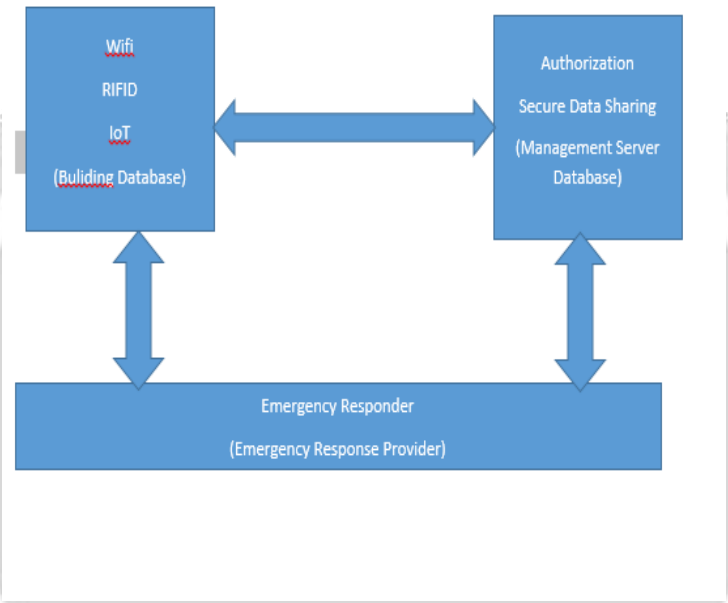

Fig. 2 System Architecture

5. REQUIREMENTS AND CHALLENGES

We identify major requirements for the user to actually Control how the data entering her personal digital space is collected, protected, shared and finally used.

5.1 **Controlled collection of sensed data:**

The targeted user(s) should be the unique recipient(s) of raw sensed data and would accept externalizing only aggregates by opting in for selected applications.

Related challenges: Co-design is a primary issue to allow the Definition of affordable sensor-based trusted cells. Low-cost is indeed a prerequisite to the generalization of trusted sources, Capable of securely filtering and aggregating stream-based spatiotemporal data with tiny hardware resources. Some trusted source being weakly connected to the Internet; asynchrony problems must also be addressed. Finally, the combination of data streams from multiple sources, each being separately harmless, may generate new privacy risks that must be carefully tackled.

5.2 **Secure private store:**

All data must be made highly available, Resilient to failure and protected against confidentiality and Integrity attacks. Accessing this data from any terminal, including those outside the user's ownership sphere (e.g., internet café), should leave no trace of the access.

5.3 **Secure sharing:**

The user can decide to keep her data private or share it with other users or group of users under certain conditions (e.g., time, location). Under which model the access control policies are actually defined is an open issue, but not the main concern of this paper. However, we insist that the user must get a proof of legitimacy for the credentials exposed by the participants of a data exchange and must trust the evaluation of the exchange conditions. Practically, sharing data means sharing the associated metadata

5.4 **Shared Commons:**

Privacy has also a collective dimension in the sense that preserving one's privacy should not hinder societal benefits (e.g., census, epidemiologic releases, and global queries). A trusted cell user is thus expected to participate to global treatments assuming her data suffers appropriate transformations (e.g., anonymization, output perturbation) depending on the trustworthiness of the recipient(s) and the expected usage of the data/query. When data needs to be transformed before being delivered, the recipient trusted cell implements the transformation on its own if possible (e.g., filtering, local data perturbation) or in collaboration with other trusted cells if the transformation requires a collective action (e.g., anonymization, global data perturbation).

6. CONCLUSION

We have presented the proof of concept for a context-aware emergency response system in a smart city. An architecture that allows sharing of critical information between various parties in order to facilitate effective first response is developed. This is done while addressing the issues of data security and privacy that arise from dissemination of such sensitive information.

7. REFERENCES

[1] Towards Cloud based Smart Cities Data Security and Privacy Management, IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014
[2] Trusted Cells: A Sea Change for Personal Data Services
[3] The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible
[4] User-Defined Privacy Grid System for Continuous Location-Based Services
[5] See Through Walls with COTS RFID System!
[6] Nuzzer: A Large-Scale Device-Free Passive Localization System for Wireless Environments
[7]http://www.firstresponder.gov/SitePages/Technology/Profile.aspx?s=Technology&itemID=15
[8] https://azure.microsoft.com/en-us/documentation/services/multifactor-authentication/