Mobile Sensor Cloud Computing

Controlling and Securing Data Processing Over Smart Environment through Mobile Sensor Cloud Computing (MSCC)

Ranbijay Kumar
PhD Student, Department of CSE
SCSVMV University
Kanchipuram, Tamilnadu, India
kumar.ranbijay@gmail.com

Dr. S. Rajalakshmi
HOD, Department of CSE
SCSVMV University
Kanchipuram, Tamilnadu, India
raji.scsvmv@gmail.com

Abstract— **The concept of Mobile Sensor Cloud Computing (MSCC) is to extend Sensor cloud-computing ecosystem to the world of future sensor enabled mobile applications and Internet clouds. Also it introduces new technologies, hardware, software, communication protocols, etc., which together forms ecosystem of mobile cloud. Smart world environment that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network. Wireless Sensor Networks (WSN) solutions, a growing green movement, demand for public safety solutions. WSN offer a powerful combination of distributed sensing, computing and communication. WSN have very high resource constraints in terms of memory, processing, and transmission power. They lend themselves to countless applications and, at the same time, offer numerous challenges due to their peculiarities. This paper includes an overview of wireless sensor networks, integration of sensor cloud computing services in smart city environment and accessible the same through sensor intended mobile. Also, it covers a comprehensive study regarding the requirements, different kind of well-known attacks and some of the proposed solution and model to counter the security attacks on WSN.**

Keywords- wireless sensor network; cloud computing; mobile cloud computing; smart environment; sensor cloud; mobile data protection

I. INTRODUCTION

Sensor networks are keys to the creation of *smart environments,* which embed information technology in everyday home, cities and work environments. The increasing interest in wireless sensor networks can be promptly understood simply by thinking about what they essentially are: a large number of small sensing self-powered nodes which gather information or detect special events and communicate in a wireless fashion, with the end goal of handing their processed data to a base station. Sensing, processing and communication are three key elements whose combination in one tiny device (mobile and tablet) gives rise to a vast number of applications. Sensor networks provide endless opportunities, but at the same time pose formidable challenges, such as the fact that energy is a scarce and usually non-renewable resource. However, recent advances in low power VLSI, embedded computing, communication hardware, and in general, the convergence of computing and communications, are making this emerging technology a reality. Likewise, advances in nanotechnology and Micro Electro-Mechanical Systems (MEMS) are pushing toward networks of tiny distributed sensors and actuators [4].

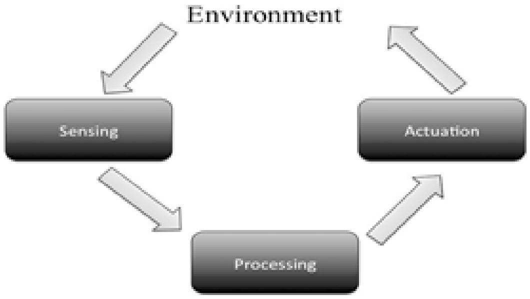

Fig1. Sensor Network Systems

Sensor networks offer economically viable solutions for a variety of applications. For example, current implementations monitor factory instrumentation, pollution levels, free- way traffic, and the structural integrity of buildings. Other applications include climate sensing and control in office buildings and home environmental sensing systems for temperature, light, moisture, and motion.

As IT delivery methods meet the demand for the use of cloud services, communicative devices and employee-owned devices, new software vulnerabilities will be introduced, and financially motivated attackers will develop innovative attack paths. The combination of new vulnerabilities and more targeted attacks will lead to continued growth in bottom-line financial impact because of successful cyber-attacks. Cyber-attacks against mobile platforms, especially smartphones,

978-0-7695-5125-8/13 $26.00 © 2013 IEEE
DOI 10.1109/CSA.2013.166

IEEE computer society

grew in 2010 and continuing with the subsequent years according to the recent *Threat Quarterly Report* published by the Threat IT Labs. The need to understand the threats and what to do about them is obvious given the current ongoing boom in the convergence of sensor enabled mobile platforms and cloud computing that defines mobile cloud computing role into the smart environment. This evolving threat environment is having an impact on some businesses and smart spaces.

This paper addresses security and control approach in respect of the mobile wireless sensor networks (MWSN), cloud computing and existing sensor devices by looking at the current state of security attacks in the cloud [23], vulnerabilities of mobile cloud ecosystems, behavior of the existing sensor devices and how those vulnerabilities are being addressed. Future issues for securing and controlling the smart environments (i.e., smart city, smart home, other smart work environment) though mobile cloud computing ecosystem are also discussed, and also discussed the opportunities for developers; service providers and operators are noted in aspect of providing solutions for existing issues.

II. SMART ENVIRONMENT KEY ASPECTS AND SECURITY THREATS IN RESPECT OF SENSOR CLOUD

WSNs provide unique opportunities of interaction between computing devices and their environment. The adhoc nature and wireless vulnerability make WSN a soft target for security attacks. In order to understand the security aspects of WSN in context of smart environment, we provide a brief description of the different attacks, existing behavior around the sensors and then present the possible solutions.

Let's start with little understanding of the *smart environment* concepts which is possible to achieve based on the knowledge of smart sensors, sensor networks and of-course the process of information flow among the environments [3]:

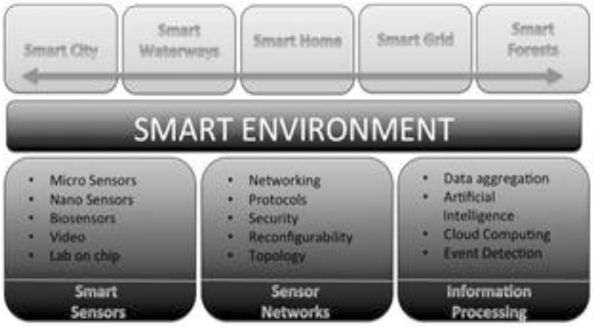

Fig2. Smart Environment

A. *Cloud is Limited – as of now*

- The immense power of the cloud can only be fully exploited if it is seamlessly integrated into our physical lives.

B. *Wireless Sensor Networks (WSNs)*

- Seamlessly couples the physical environment with the digital world. Sensor nodes are small, low power, low cost, and provide multiple functionalities, such as, Sensing capability, processing power, memory, communication bandwidth, and battery power.

B. *Sensor Networks are Limited too*

- It's very challenging to scale sensor networks to large sizes. Operate in separate silos. Sensor data cannot be easily shared by different group of users.
- Insufficient computational and storage resources to handle large-scale application (i.e., in smart cities and environment)
- Used for fixed and specific applications that cannot be easily changed once deployed. Slow adoption of large-scale sensor network application.

C. *Integrate Sensors with Cloud – Smart Environment*

Smart clients use services from cloud [4]. Cloud stores data, registers data streams and data events. Following are the key expectation when sensors integrate with cloud services to access data for smart clients:

- Acquisition of data feeds from numerous physical area (city, home, waterways, etc.) and wide area (water quality, weather monitoring, traffic signal, etc.) sensor networks in real time.
- Real-time processing of heterogeneous data sources in order to make critical decisions.
- Automatic formation of workflows and invocation of services on the cloud one after another to carry out complex tasks.
- Highly swift data processing using the immense processing power of the cloud to provide quick response to the user.

E. *Mobile Sensors*

Modern smartphones have a variety of in-built sensors to detect, for example, movement, orientation, rotation, proximity, temperature and magnetic fields. The camera, the most widely used sensor on a phone, allows a device to "see" the outside world, while the microphone lets the device "hear." And many devices now have multiple cameras and microphones for possible spatial resolution. Other means to let a device "see" include light and proximity sensors. The ability to "hear" is further facilitated by any of the four wireless sensors (cell tower, Wi-Fi, Bluetooth, and GPS). Considering these communication devices as sensors naturally leads to methods of determining context, and providing an overall "sense" of the world around the device. The advanced and latest smartphone phone includes eight different sensors: accelerometer, GPS, ambient light, dual microphones, proximity sensor, dual cameras, compass, and gyroscope [1].

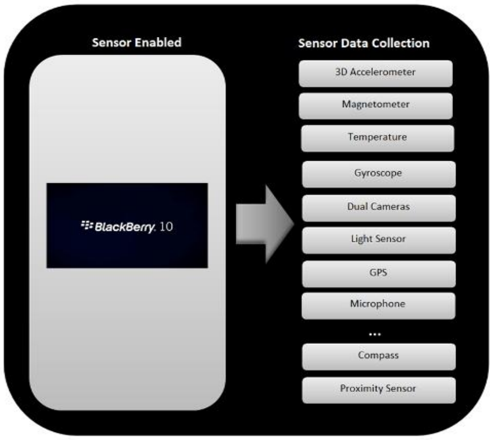

Fig3. Suite of Sensors in Advanced Smartphone

E. Attacks against Sensor Privacy:

Sensor networks provide increased data collection capabilities. Some of the more common attacks [19, 22] against sensor privacy are:

- *Monitor and Eavesdropping* This is the most obvious attack to privacy. By listening to the data, the adversary could easily discover the communication contents.
- *Traffic Analysis* Traffic analysis typically combines with monitoring and eavesdropping.

III. CHALLENGES AND PROBLEMS INVOLVED IN SENSOR CLOUD WHICH AFFECTS THE PERFORMANCE OF SMART ENVIRONMENT

Sensors networks in general pose considerable technical problems in data processing, communication, and sensor management. We cannot deploy such a critical technology, however, without first addressing the security and privacy research challenges to ensure that it does not turn against those whom it is meant to benefit [2, 4].

A. Technical and Research Challenges:

1. *Complex Event Processing and Management*
   - Real-time data feeds from heterogeneous sensors trigger certain events and services.
2. *Massive Scale and Real Time Data Processing*
   - Integration with heterogeneous and massive data sources is a challenge due to the amount of information to be mined and used in real time.
3. *Large Scale Computing Frameworks*
   - Multiple sensor data sets used for decision making may or may not be collocated. If these data sets and their corresponding access/search services are geographically distributed, the allocation of computational and storage and data migration become critical challenges.
4. *Harvesting Collective Intelligence*
   - Heterogeneous and real-time sensor data feeds allow us to improve the decision making by using data and decision level fusion techniques.
   - To maximize the intelligence that can be exploited from massively collocated information in a cloud is a challenge.

B. Additional challenges

a) The overall system is very volatile
   - Changes in environment conditions can render readings inaccessible.
   - Failure of nodes cannot be easily fixed.
   - Nodes can run low on power over time.

b) Data is dynamic.
   - New data is being appended all the time, cause for the power consumption.

c) Serving multiple queries concurrently is problematic.
   - Sensors are very limited on physically what they can observe at a given time.

IV. PROTECTING AND SECURING MSCC ECOSYSTEMS FROM CURRENT AND FUTURE THREATS

The privacy and security issues posed by sensor networks represent a rich field of research problems. Improving network hardware and software may address many of the issues, but others will require new supporting technologies. Some of exists effective techniques to counter many of the attacks levied against a sensor are addressed here in respect of security and privacy; they are [2, 5, 7, 8, and 9]:

1. Anonymity Mechanisms:

Total anonymity is a difficult problem given the lack of knowledge concerning a node's location. Therefore, a tradeoff is required between anonymity and the need for public information when solving the privacy problem. In [18, 19, 20, and 21], three main approaches are proposed:

- *Decentralize Sensitive Data* the basic idea of this approach is to distribute the sensed location data through a spanning tree, so that no single node holds a complete view of the original data.

- *Secure Communication Channel* using secure communication protocols, such as SPINS [65], the eavesdropping and active attacks can be prevented.

- *Change Data Traffic* De-patterning the data transmissions can protect against traffic analysis.

- *Node Mobility* making the sensor movable can be effective in-defending privacy, especially the location. For example, the Cricket system [67] is a location-support system for in-building, mobile, location dependent applications. It allows applications running on mobile and static nodes to learn their physical location by using listeners that hear and analyze information from beacons spread throughout the building. Thus the location sensors can be placed on the mobile device as opposed to the building infrastructure, and the location information is not disclosed during the position determination process and the data subject can choose the parties to which the information should be transmitted.

2. *Policy-based Approaches:*

Policy-based approaches are currently a hot approach to address the privacy problem.

- The concept of private authentication, and give a general scheme for building private authentication with work logarithmic in the number of tags in (but not limited by) RFID (radio frequency identification) applications.

- *Snekkenes* [24] presents advanced concepts for specifying policies in the context of a mobile phone network. These concepts enable access control based on criteria such as time of the request, location, speed, and identity of the located object.

- Myles and colleagues [25] describe Architecture for a centralized location server that controls access from client applications through a set of validator modules that check XML/JSON-encoded application privacy policies.

2. *Information Flooding:*

Based on flooding-based routing protocols, Ozturk et al. have developed comparable methods for single path routing to try to solve the privacy problems in sensor network.

- *Baseline Flooding* In the baseline implementation of flooding, every node in the network only forwards a message once, and no node retransmits a message that it has previously transmitted. When a message reaches an intermediate node, the node first checks whether it has received and forwarded that message before. If this is its first time, the node will broadcast the message to all its neighbors. Otherwise, it just discards the message.

- *Probabilistic Flooding* in probabilistic flooding, only a subset of nodes within the entire network will participate in data forwarding, while the others simply discard the messages they receive.

- *Flooding with Fake Messages* This observation suggests that one approach to alleviate the risk of source-location privacy breaching is to augment the flooding protocols to introduce more sources that inject fake messages into the network.

- *Phantom Flooding* Phantom flooding shares the same insights as probabilistic flooding in that they both attempt to direct messages to different locations of the network so that the adversary cannot receive a steady stream of messages to track the source.

- Another strategy used to mask location information from *eavesdroppers* is presented in [26]. They propose a two way greedy random-walk strategy GROW (Greedy Random Walk).

V. PROPOSED SOLUTIONS AND APPROACH

. *Fundamental Approaches:*

Collect all the sensor data to one or more data centers [4]

a) Use a classical DBMS

- Energy inefficiencies due to redundant data collection, central point of failure, hot spots near root, has to collect data at the highest frequency for all potential queries and all the time

b) Rebuild a DBMS for sensor networks - fix some of the problems on a central setting

- Still energy inefficient due to centralization
- In-network storage and processing along with a capability to inject and collect data from anywhere in the network for any number of centers
- But storage limitations require eliminating some data

c) Execution Steps

- Broadcast the query to the network Collect data back Note: Either a human or an automated system can be the origin of the query

d) Storing Data versus Data Collection

- Rather than collecting data from individual sensors for every given query, sensors can be made to store their data in the network for *point* retrieval at a later time

A. The Sensor Cloud

- An infrastructure [4, 11, 14] that allows truly pervasive computation using sensors as interface between physical and cyber worlds, the data-compute clusters as the cyber backbone and the internet as the communication medium.
- It integrates large-scale sensor networks with sensing applications and cloud computing infrastructures.
- It collects and processes data from various sensor networks.
- Enables large-scale data sharing and collaborations among users and applications on the cloud.
- Delivers and controlled cloud services via sensor-rich mobile devices.
- Allows cross-disciplinary applications that span organizational boundaries.
- Enables users to easily collect, access, process, visualize, archive, share and search large amounts of sensor data from different applications.
- Vast amount of sensor data can be processed, analyzed, and stored using computational and storage resources of the cloud.
- Enables sensor devices to handle specialized processing tasks.

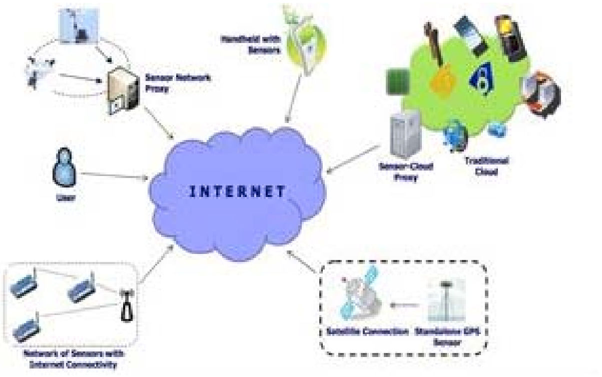

Fig4. Sensor Cloud Architecture (SCA)

B. MSCC Architecture [10, 11, 12, 13] *:*

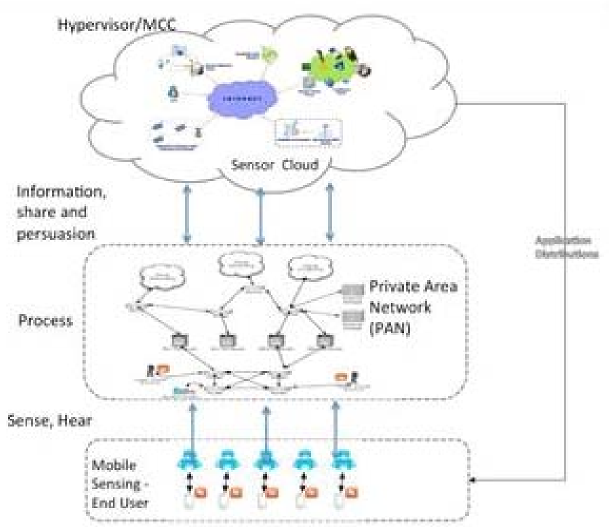
Hypervisor/MCC
Sensor Cloud
Information, share and persuasion
Process
Private Area Network (PAN)
Sense, Hear
Mobile Sensing - End User
Application Distributions

Fig5. Mobile Sensor Cloud Computing (MSCC) Architecture

VI. OBJECTIVES AND KEY IDEAS

WSN's is a specific technology that helps to create Smart space (smart cities, smart grid, smart building, etc.) [3, 15]. The aim is to create a distributed network of intelligent sensor nodes, which can measure many parameters for a more efficient management of the city.

In context of smart city we have few examples, citizens can monitor the pollution concentration in each street of the city or they can get automatic alarms when the radiation level raises a certain level. It is also possible for the authorities to optimize the irrigation of parks or the lighting of the city. Water leaks can be easily detected or noise maps can be obtained. Rubbish bins can send an alarm when they are close to being full.

Vehicle traffic can be monitored in order to modify the city lights in a dynamic way. Traffic can be reduced with systems that detect where the nearest available parking slot is. Motorists get timely information so they can locate a free parking slot quickly, saving time and fuel. This information can reduce traffic jams and pollution improves the quality of life.

By 2015, more than 240 million business customers will be leveraging cloud-computing services through mobile devices, driving revenues of $5.2 billion.

Key features of our interest to achieve into the smart environment [16] scenario:

- Immense computational and storage resources that are collocated
- Accessibility over the Internet with high speed access

- Accessibility from virtually any platform and device

To achieve all features in aspect of *smart client* must have to be focus on the following key components:

1. *Sensor-Cloud Proxy (SCP)*

- Interface between sensor resources and the cloud fabric. It manages sensor network connectivity between the sensor resources and the cloud.
- Exposes sensor resources as cloud services.
- Uses cloud discovery services for resource tracking.
- Manages data from sensor networks
    - − Data format conversion into standard formats (e.g. *XML, JSON*)
    - − Data cleaning and aggregation to improve data quality
    - − Data transfer to cloud storage in secure manner (i.e., *encrypted data*)

2. *Sensor Network Proxy (SNP)*

- The sensor network is still managed from the *sensor-cloud* interface via *sensor network proxy*
- The proxy collects data from the sensor network continuously or as and when requested by the cloud services.

2. *Accessing Device Sensor's in BlackBerry 10*

Steps need to follow up and understand before jump into the mobile client-side program for controlling the smart space via sensors [28]:

a) *Sensor Management*

The sensor management package is a standard application that provides sensor management services to other applications on the device. This provides the BlacBerry10 device user and client applications with an interface to list installed support packages and invoke them in limited ways.

b) *Sensor Support Packages*

Individual sensor support packages provide the features necessary to interface with a specific sensor or set of sensors.

c) *Sensor Availability*

Each sensor support package and permissions is required to implement. MUST NOT abort any broadcast it receives.

d) *Sensor Communication*

Each sensor support package will handle all communication details with the actual sensor.

e) *Sensor Configuration*

Each sensor support package will implement an interface to view and change the individual sensor's configuration. This interface will handle all communication with the sensor and will provide an interface specific to the individual sensor.

f) *Sensor Sampling & Capture*

Each sensor support package will implement an interface to capture samples from supported sensors

g) *Sensor Capture Viewing*

Each sensor support package will implement an Android Activity that will provide an interface to view a sample capture from the specific sensor.

h) *Sensor Identification*

A standard way of identifying sensor types and specific sensors (including communication information) is required: this ensures that new applications will be able to use the sensor support system and new sensors can be cleanly added to the system.

i) *Sensor Type Identification*

The sensor type identification scheme builds upon the mime-type support already present in the mobile application programming model. All sensors are identified using a basic mime-type of *application/vnd.sensor.{sensor type}.{variant}*

j) *Sensor Selection and Communication Channel Identification*

The sensor selection and communication channel identification is built on the URI handling system already present in the mobile programming model. Sensors may use different communication channels to interact with the blackberry device: the nominal default communication channel is Bluetooth, but it is entirely possible to model internal

Programmatically in BlackBerry10:

Also, we are going to see here, how to access sensor enabled API's in BlackBerry device and retrieve data from it [27].

```
main.qml:
import bb.cascades 1.0
import QtMobility.sensors 1.2
TabbedPane {
  id: tabPane
  showTabsOnActionBar: true
  onCreationCompleted: {
        OrientationSupport.supportedDisplayOrientation =
SupportedDisplayOrientation.All;
        tabPane.activeTab = compassTab;
    }
/* Block of statements for other tabs such as Motion
Alarm, Compass, Flashlight, Motion Alarm and Collision
Detector.*/
Tab {
        id: rotation3DTab
        title: qsTr("Rotation 3D")
        imageSource: "images/rotation3d.png"

        Page {
            ControlDelegate {
                source: "rotation3D.qml"
                delegateActive: (tabPane.activeTab ==
rotation3DTab)
            }
        }
    }
}
```

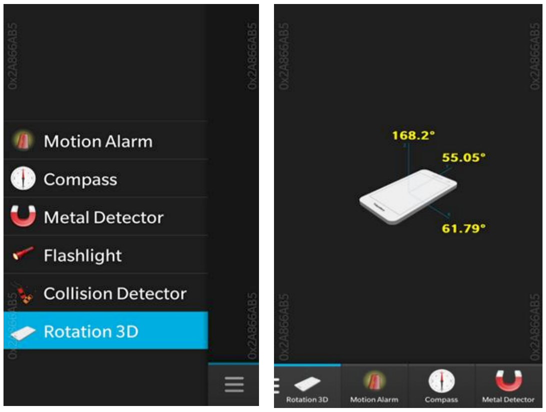

Fig6. Sensor Demo UI view in BlackBerry10

VII. FUTURE AND SCOPE OF MSCC

Sensor device and sensor network technologies will be presented along with their key applications onto smart buildings, home energy management systems, intelligent city transportation systems, urban precision agriculture, city environment, etc. As more mobile devices enter the market and evolve, certainly security issues will grow as well. New applications which are designed for mobility from the ground up and utilize location awareness, cloud sensors services, and access to big data driven decision-making systems will force companies to restructure around the idea of mobility as the norm [3, 15].

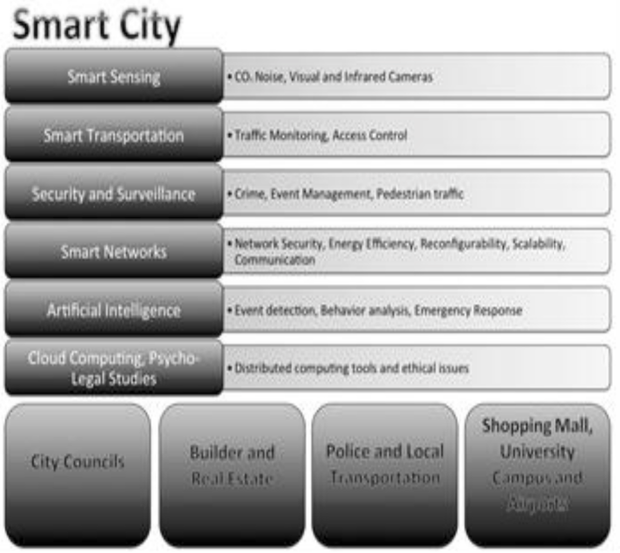
Smart City
Smart Sensing
• CO, Noise, Visual and Infrared Cameras
Smart Transportation
• Traffic Monitoring, Access Control
Security and Surveillance
• Crime, Event Management, Pedestrian traffic
Smart Networks
• Network Security, Energy Efficiency, Reconfigurability, Scalability, Communication
Artificial Intelligence
• Event detection, Behavior analysis, Emergency Response
Cloud Computing, Psycho-Legal Studies
• Distributed computing tools and ethical issues
City Councils
Builder and Real Estate
Police and Local Transportation
Shopping Mall, University Campus and Airports

Fig7. Smart City Realization as Internet of Things

One possible trend is incorporation of hypervisors into smartphones. A *hypervisor* is a program that allows multiple operating systems to share a single computer. This development is intended to simplify smartphone management problems. It also has potential to simplify security management.

Another trend is the growth of what is known as the *Internet of Things*. The growth in intelligent devices that are able to interact with the Internet is growing at a much greater rate than traditional computer technology.

These are the trends arising over recent years that are changing the way developer and expert's work. Some recent key trends are:

- *Mobility* – Mobile devices are being increasingly used for access to corporate data and smart environment. So, it's necessary to improve sensor enabled mobile OS in the following aspect
- *More virtual sensors*- the most cost effective way of supporting growing infrastructure requirements.
- *Endless Data Growth* – the many different ways of accessing and using information are leading to an explosion in the amount of data stored.
- Performance evaluation and modeling of mobile and wireless networks (MWSN)
- Testing and debugging techniques for MSCC systems

VIII. CONCLUSION

Mobile cloud computing is poised to become a huge market. That huge market will attract the attention of criminals who want to make an easy profit by finding and exploiting weaknesses in mobile cloud ecosystems. Also, enormous growth in the variety of devices connected to the Internet will further drive security needs. This paper presented some of the issues that are pertinent for planning how to provide security for the WSN's and discussed about sensor cloud services in the context of mobile cloud computing and also focuses on the several challenges related to MSCC ecosystems in current or in near future practice.

As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications. In particular, the addition of mobile sensing and sensor cloud computing services will likely make strong security a more realistic expectation in the future. We also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas especially in the terms of *smart environment*. However, technical challenges of WSNs need to be addressed jointly by mobile application developers, researchers, wireless network service providers and IT departments, as this will be primarily determined by the network providers based on profitability, potential security vulnerabilities and user acceptance.

References

[1] Nicholas D. Lane, Emiliano Miluzzo, Hong Lu, Tanzeem Choudhury, and Andrew T. Campbell, "Ad Hoc And Sensor Networks: A Survey of Mobile Phone Sensing".

[2] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey".

[3] M. Palaniswami, "ISSNIP: Towards Sustainable Smart Cities – Role of Large Scale WSNs".

[4] Ramamohanarao (Rao) Kotagiri, Egemen Tanin, Lars Kulik, Palaniswami, "Sensor Networks and Related Research Issues".

[5] Chee-Yee Chong, and Srikanta P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges".

[6] Daniele Puccinelli, and Martin Haenggi, "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing.

[7] Haowen Chan, and Adrian Perrig, "Security and Privacy in Sensor Networks".

[8] Arjit Ukil, "Security and Privacy in Wireless Sensor Networks".

[9] Apu Kapadia, Steven Myers, XiaoFeng Wang, and Geoffrey Fox,"Secure Cloud Computing with Brokered Trusted Sensor Networks".

[10] Dr Lim Hock Beng, "Sensor Cloud: Towards Sensor-Enable Cloud Services".

[11] Adam Dunkels, "Smart Cities and IP-Based Sensor Networks: A Conversation with Adam Dunkels".

[12] Martin Haenggi, "Wireless Sensor Networks: A New Paradigm for Ubiquitous Sensing and Information Processing".

[13] http://blog.blrdroid.org/2012/01/sensors-and-location-based-services/

[14] Mukundan Sridharan, Rajiv Ramnath, Emre Ertin, and Anish Arora, "Mobility Centric Campus Area Sensor Network for Locality Specific Applications".

[15] Luis M. Correia, and Klaus Wunstel, "Smart Cities Applications and Requirements".

[16] Yang Peng, Zi Li, Wensheng Zhang, and Daji Qiao, "Prolonging Sensor Network Lifetime Through Wireless Charging".

[17] Mohsen Sharifi, Saeed Sedighian, and Maryam Kamali, "Recharging Sensor Nodes Using Implicit Actor Coordination in Wireless Sensor Actor Networks".

[18] M. Gruteser and D. Grunwald. A methodological assessment of location pri- vacy risks in wireless hotspot networks. In First International Conference on Security in Pervasive Computing, 2003.

[19] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald. Privacy-aware lo- cation sensor networks. In 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX), 2003.

[20] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location- support system. In Proc. of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MOBICOM), August 2000.

[21] A. Smailagic, D. P. Siewiorek, J. Anhalt, and Y. Wang D. Kogan. Location sensing and privacy in a context aware computing environment. In Pervasive Computing, 2001.

[22] H. Chan and A. Perrig. Security and privacy in sensor networks. IEEE Com- puter Magazine, pages 103–105, 2003.

[23] Sophos, "Security threat report 2011".

[24] E. Snekkenes. Concepts for personal location privacy policies. In Proceedings of the 3rd ACM conference on Electronic Commerce, pages 48–57. ACM Press, 2001.

[25] G. Myles, A. Friday, and N. Davies. Preserving Privacy in Environments with Location- Based Applications. IEEE Pervasive Computing, 2(1):56–64, 2003.

[26] http://devblog.blackberry.com/2012/11/blackberry-10-mobile-sensing/, Ranbijay Kumar (RAN), 2012.

[27] Y. Xi, L. Schwiebert, and W. Shi. Preserving privacy in monitoring-based wireless sensor networks. In Proceedings of the 2nd International Workshop on Security in Systems and Networks (SSN '06), IEEE Computer Society, 2006.

[28] http://www.androidcompetencycenter.com