eSAME 2015 Conference

Sensors on mobile devices – applications, power management and security aspects

Katrin Matthes[1)], Rajasekaran Andiappan[2)], Intel Corporation

[1)]Sophia-Antipolis, France [2)] Espoo, Finland

Abstract: *Mobile devices, in particular smartphones, have an increasing number of sensors attached to them. There are different categories of sensors such as motion, environmental, location/position, etc. Inputs of several sensors may be combined to deliver more accurate results to applications.*
While applications get richer thanks to new sensors (e.g. in the domain of health) there is also increased power consumption of the mobile device linked to the continuous sensing that has to be dealt with.
On top of that the mobile devices collect potentially sensitive information about the user that need to be protected.
This paper covers the some new applications and services that are enabled through sensors and sensor fusion, as well as a system architecture for low power always ON sensing combined with a security architecture to protect sensitive user data.

I. Introduction

The number of sensors and their usage has significantly increased in mobile devices over the past years. In addition to "classical" sensors such as accelerometer, gyrometer, magnometer and pressure sensors that are used to determine device orientation, mobile gestures, and context awareness in general, mobile devices incorporate a variety of sensors for health and fitness such as heartrate, UV and air pollution.
Mobile devices are now aware of our activity, location and environment, by continuously acquiring data from the attached sensors and by fusing together sensor data (this is also referred to as "Always On context Awareness").
Applications can use either raw sensor data or fused (i.e. intelligently combined data), the computed output can be stored locally or in the cloud.
The increased use of sensors in mobile devices generating continuously data to process at increased sampling rates (such as location and itineraries, activity and activity context, health, etc.) brings new requirements linked to the acquisition, processing and storage of the sensor data.
These requirements include low power consumption and data protection from unauthorized access.

The Intel® Integrated Sensor Solution has been designed to improve user experience enabling applications with additional context processing and cloud support while maintaining battery life thanks to low power architecture.

II. Intel® Integrated Sensor Solution

The Intel® Integrated Sensor Solution consists of an Integrated Sensor Hub in the Intel SoC designed for low power and platform BOM cost optimization and software including sensor algorithms and fusion with context processing.

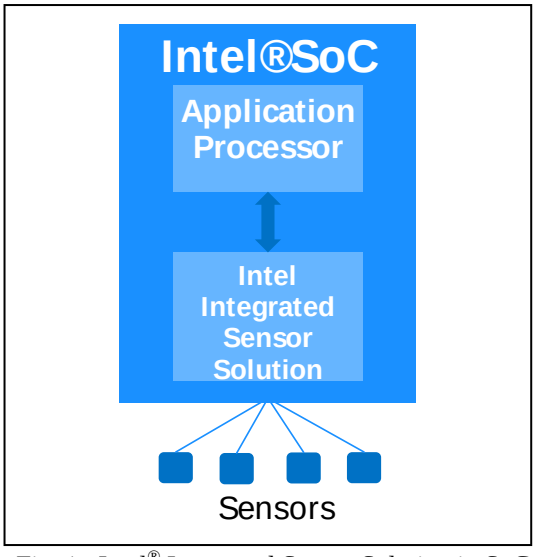

Fig. 1. Intel® Integrated Sensor Solution in SoC

A. Hardware Architecture

The Integrated Sensor Hub (ISH) is integrated in the SoC. It is composed of a low power microprocessor, internal memory, I/Os for connection of sensors and fabric for communication with the Application Processor or Main CPU and other IPs embedded into the SoC.

The heart of the ISH is a X86 CPU running at 100Mhz. The memory includes 32 KB L1$, 8 KB ROM and 640 KB SRAM. Low speed IO ports (sensor interface controllers) are I2C, SPI, UART, GPIO.

In addition there is a power management and clocking unit as well as a debug interface. The HW architecture is depicted in Fig.2.

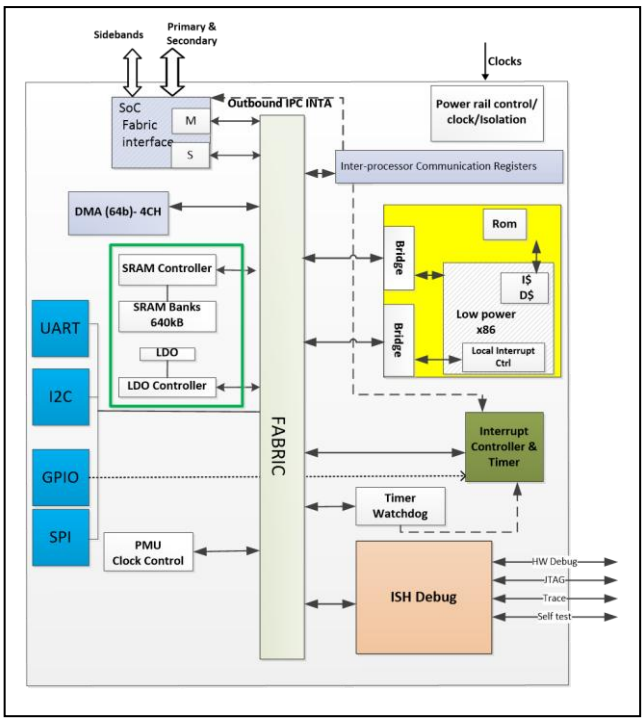

Fig. 2. Integrated Sensor Hub Architecture

B. *Power Management*

The ISH is designed as an autonomous sub-system that can operate while the rest of the SoC is in low power mode.

The active power consumption of the ISH is comparable to the SoC retention and sleep power (estimated for a CPU running at 100 MHz with 32kB of L1 cache and 640 kB of SRAM for code and data storage). This means that continuous sensing through the ISH (sensor data acquisition, sensor algorithms and capable of fusion) can be performed with no or very minimal impact to the battery life of the mobile device.

The ISH autonomously manages its power states, depending on the sensor sampling frequency and the time between processing of sensor data in general. D0 is the active state during which the ISH processes workloads. D0i1, D0i2 and D0i3 are idle states with wake latencies of 10 us, <100 us and <3 ms, respectively. In D0ix idle states ISH internal logic is put into low power mode (CPU in HALT state, memory logic clock gated, in retention or power gated, etc.). The deeper the power state, i.e. the more logic including memories is in low power mode, the higher the time the wake latency (in particular linked to the time to restore the memory in D0i3). All ISH device states (including the active state D0) allow the rest of the SoC to stay in deep sleep mode.

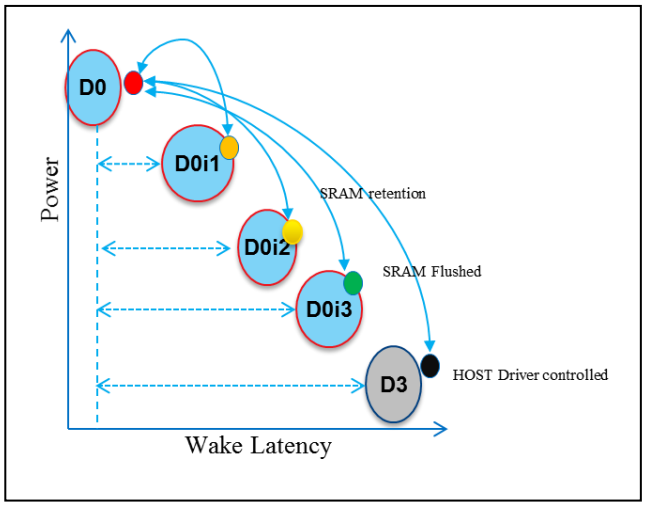

Fig. 3. ISH power states

The ISH wakes up the Application Processor through interrupt when ISH side processing is finished and the OS application has data available to process.

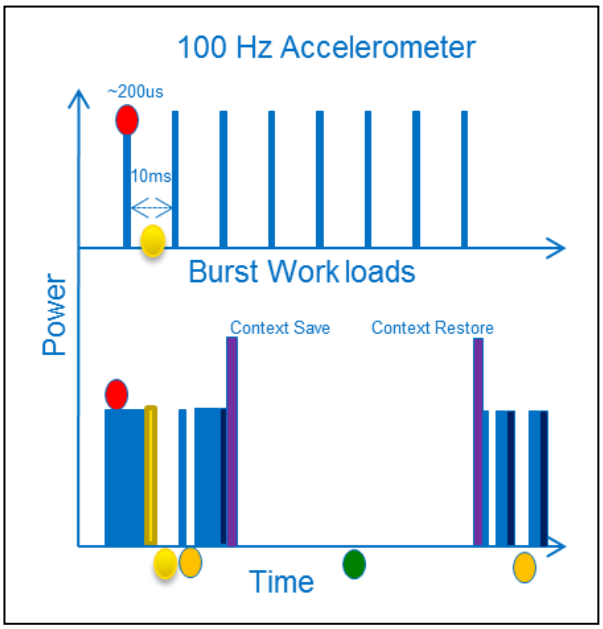

Fig. 4. Workload based Device Power State Management

The ISH autonomously manages its device based on the processing load and time between workloads. Fig. 4 gives an example of device power state management based on the workloads associated to accelerometer processing. The accelerometer is operated at 100 Hz, i.e. 10 ms sampling period. During processing intensive periods of accelerometer sensor data the ISH will go into either D0i1 or D0i2 state as the time between work load processing is low (several tenths of microseconds to several hundreds of microseconds, respectively. During sample acquisition periods with low or no processing the ISH goes into its lowest power state, D0i3. The

D0i3 state requires context save and restore as the memory is power gated and memory content lost during this state.

C. *Software and Firmware Architecture*

The Sensor related Software and Firmware stacks are part of the Intel® Integrated Sensor Solution.

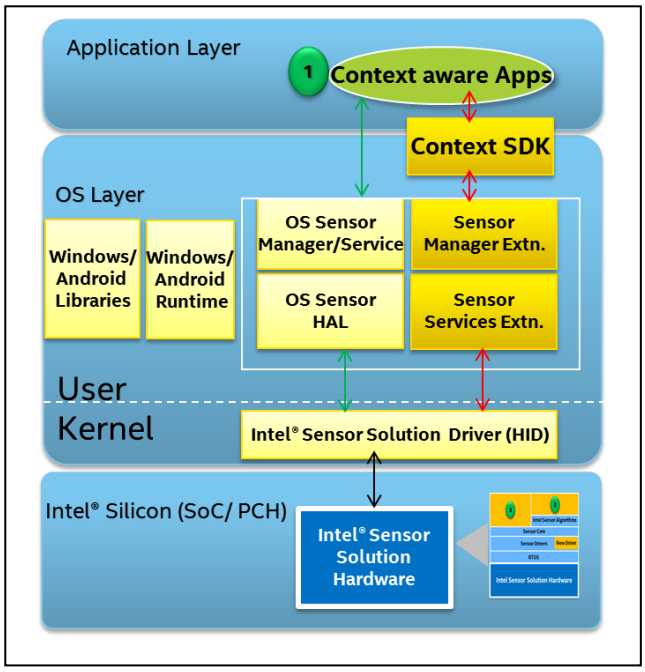

Fig. 5. Software stack on host side

The Intel® Sensor Solution software stack on host side depicted in Fig. 5 has the same partitioning for Windows and Android OS.

Intel provides solutions on three levels. The Level 1 resides at UI Level. Contextual sensing with support of advanced applications is enabled through extensions of the APIs (Application Programming Interfaces) beyond th APIs natively supported by the OS. These APIS are both client and cloud based which allows building end-to-end solutions (from capturing and processing sensor data on the mobile device to services running on servers in the cloud).

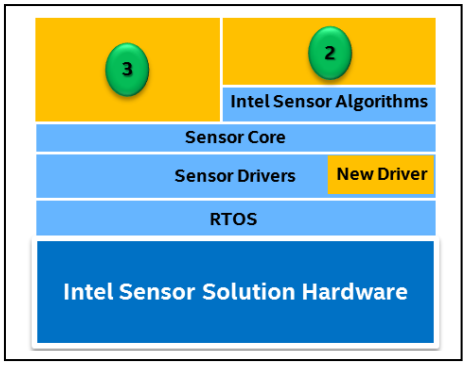

Fig. 6. Firmware stack on ISH

The lower levels of programmability for application development reside in the sensor hub firmware stack, cf. Fig. 2.

Level 2 allows to use the Intel extensions to expose additional functionality at the interface between the CPU and the sensor hub. Level 3 enables OEM to add their own IP for differentiation and innovation.

Intel supports each of these alternatives via the Context SDK for level 1 and the Intel Sensor Solutions Firmware Development Kit for 2 and 3.

III. Sensors Supported with Intel® Sensor Solution

Intel® Integrated Sensor Solution is the hub for many sensors to the system and enables "always on" sensing usages and enable new ranges of applications (e.g. in the domain of health through support of biosensors).

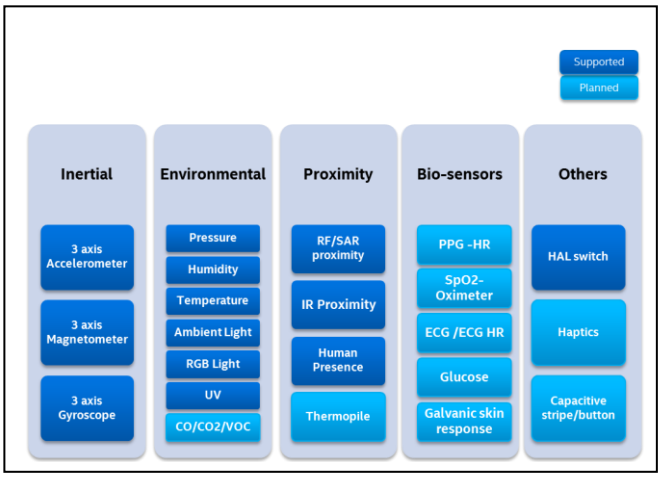

Fig. 7. Sensors supported with Intel® Integrated Sensor Solution

The integrated sensor hub, the number of sensors enables new "Always On" usages thanks to its optimized power management architecture. New applications include monitoring or heart rate, blood oxygen, glucose in the domain of health and air quality (CO, CO2, etc.) in the domain of environmental sensing.

IV. Security Aspects on the Device and in the Cloud

New types of sensors such as ECG and Glucose for health provide sensitive personal data to applications (with storage on the device or in the cloud).

Secure capture, processing and storage can be achieved on the device by using a Trusted Execution Environment (TEE).

The TEE and the Security engine form a Trusted Computing Base (TCB) that enables secure sensing. The TCB carries out software and firmware authentication. The sensor data on the device is transferred from the ISH through the security engine to the application processor using secure channels (encryption and/or certification of data).

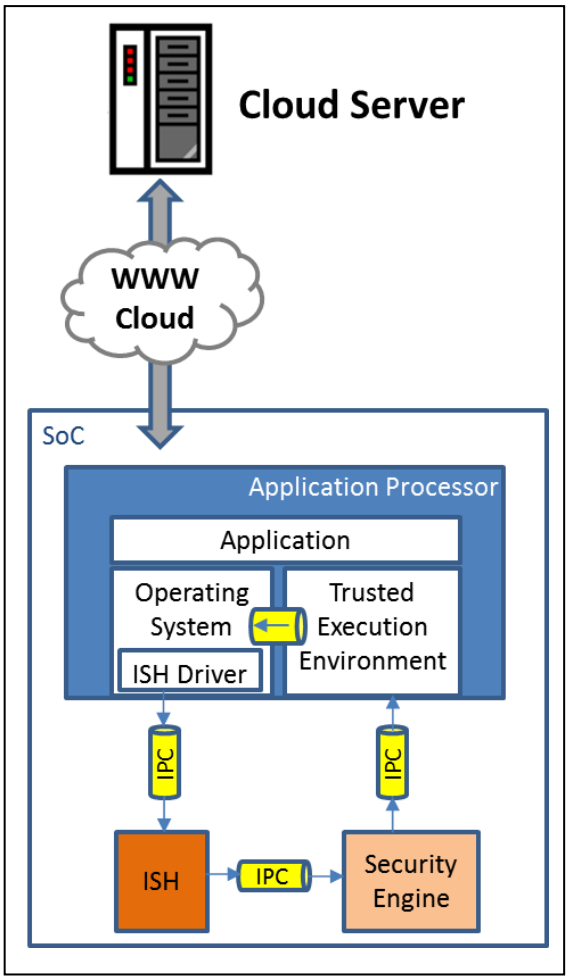

Fig. 8. Sensor data protection, device and cloud

The data also needs to be secured for transfer and processing in the cloud. Here the user enrolls with the service, establishes sign-on credentials, service generates session encryption keys so that confidential data is protected. User data aggregation (decryption, integrity check, filtering and logging) based on the HW certificate associated with the user.

Device and Cloud side user data protection is shown in Fig. 8.

V. Conclusion

Intel® Integrated Sensor Solution is the hub for many sensors to the system. Thanks to low power architecture it enables a new range of applications leveraging “always on” sensing usages for various types of sensors.

Intel security technology allows securing sensitive data on the device and in the cloud, thereby providing a holistic approach to processing and managing any type of sensor data.