IJTRET

International Journal of Trendy Research in Engineering and Technology
Volume 4 Issue 5 Proceedings of NCCETCC'20
ISSN NO 2582-0958

Proceedings of National Conference on Cutting Edge Technologies in Computing & Communications
held at Sriram Engineering College, Chennai on 6th March 2020

EMERGENCY ALERTNESS FOR DETECTING SENSOR-BASED ONSMART DEVICES

[1]S. Bhuvana,[2]T.D. Kumutha,[2]P. Rekha, [2]R. ShaluAndriya
[1]Assistant Professor, [2]Final year Student,
CSE Department of Computer Science & Engineering,
Sriram Engineering College, Chennai – 602024,Tamilnadu, India
bhupreethi@gmail.com

ABSTRACT

Nowadays, nobody in this world is ready to look what's happening around them. Even though, if any accident occurs no one cares about it. This is an intention to implement an innovative solution for this problem by developing an Accident detection System using android smart phone from the accident. This system has been developed and implemented using the heart beat sensor based mobile technology integrated with the evolving android smart phone. The application for accident detection which primarily measures the sensor x and y axis using mobile sensor. After getting the signal from sensor this system filters out the background. Then count the time between each x and y that may be an accident or not. Then the system will immediately transmit the location of the accident to the pre-configured contacts through Short Message Service (SMS). In case of an accident is occurred then the driver is prompted to respond by touch or voice in order to eliminate any false detection So the proposed system ensures that to reduce by accidents.

I. INTRODUCTION:

A smart device is an electronic device, generally connected to other devices or networks via different wireless protocols such as Bluetooth,wifi, 3G, etc., that can operate to some extent interactively and autonomously. Several notable types of smart devices are smartphones, smart cars, smart thermostats, smart doorbells, smart locks, smart refrigerators, phablets and tablets, smartwatches, smart bands, smart key chains, smart speakers and others. The term can also refer to a device that exhibits some properties of ubiquitous computing, including although not necessarily artificial intelligence.Smart devices can be designed to support a variety of form factors, a range of properties pertaining to ubiquitous computing and to be used in three main system environments: physical world, human-centered environments and distributed computingenvironments. Smart devices are typically composed of a hardware layer (including a radio that transmits signals), a network layer (through which devices communicate with each other), and an application layer (through which end users deliver commands). While the number of applications using different sensors is increasing and new devices offer more sensors, the presence of sensors have opened novel ways to exploit the smart devices. Attackers can exploit the sensors in multiple ways. They can trigger an existing malware on a device with a simple flashlight they can use a sensor

To leak sensitive information; using motion sensors, attackers can record or steal sensitive information
From other nearby devices or people. They can even transfer a specific malware using sensors as a communication channel. Such sensor based threats become more serious with the rapid growth of Apps utilizing many sensors.

II.RELATED WORK:

Smart devices have become more prevalent than before with the use of different sensors such
As user's location, keystroke information, etc. Several works have investigated the possibility of these threats and Presented different potential threats in recent years. Some interesting sensor-based threats are explained below.
One of the most common threats is keystroke inference in smart devices. When a user types in the keyboard, motion sensor readings (i.e., accelerometer and gyroscope) change accordingly. As different keystrokes yield different, but specific values in motion sensors, typing information on onscreen keyboard can be inferred from an unauthorized sensor such as motion sensor data or its patterns collected either in the device or from a nearby device can be used to

extract users' input in smart devices. Light sensor readings also change while a user types on Smart devices; hence, the user input in a smart device can be inferred by differentiating the light sensor data in normal and typing modes. The light sensor can also be used as a medium to transfer malicious code and trigger message to activate a

malware. The audio sensor of a smart device can also be exploited to launch different malicious Attacks (e.g., information leakage, eavesdropping, etc.). On the device. Cameras of different smart devices can also be used to covertly capture screenshot or video and to infer information about surroundings or user activities. GPS of a smart device can be exploited to perform a false data injection attack on smart devices and infer the location of a specific device.

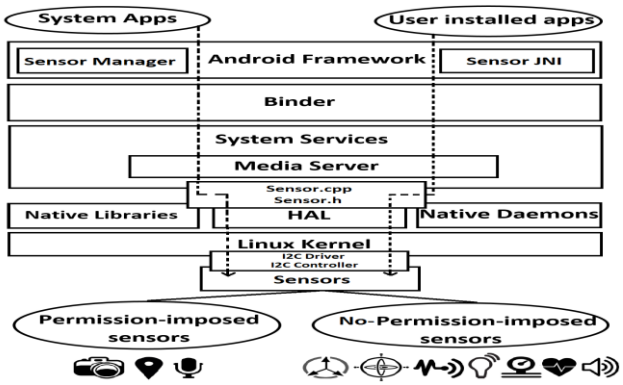
III.SENSOR MANAGEMENT IN SMART DEVICES:

Modern smart devices perform app-based operations which create a many-to-many relationship between sensors and Apps. Smart devices use more than one sensor to perform a task and hence, it is impractical to install an independent Management system for each sensor. Smart device operating systems (OS) address this requirement by implementing Centralized sensor management systems to manage and ensure secure data acquisition from all the sensors. In this Section, we discuss sensor management systems of smart device uses and articulate important deficiencies of the Existed sensor management systems.

Sensors in Smart Devices: Most of the current smart device uses offer permission-based sensor management system to control sensor access and data flow. According to the associated permissions imposed by the uses, sensors in smart devices can be categorized in two groups - permission imposedand no permission-imposed sensors.

Permission-imposed Sensor (PS): Permission-imposed sensors are those which need explicit user permission to be accessed by an App. In smart devices, GPS, camera, and microphone are considered as permission-imposed Sensor.

No Permission-imposed sensors (NPS): No-permission imposed sensors can be defined as sensors that do not
Need any user permission explicitly to be accessed by an App. Smart devices can have a wide range of no permission-imposed sensors such as accelerometer, gyroscope, proximity sensor, light sensor, etc.



IV.EXISTING METHODOLOGY:

Design and development of a prototype of an electronic gadget which is used to detect fall among elderly and the patients who are prone to it. In this article, the body posture is derived from change of acceleration in three axes, which is measured using triaxle accelerometer.state-of-the-art wearable fall detection algorithm. Detection algorithm depends mainly on the body posture and tilt, then torso is more suitable place. Stefano Abbate et al. listed different possible anatomical positions to derive various postures.

DRAWBACKS:

- It is separate device difficult to use every day
- Less accuracy.

V.PROPOSED METHODOLOGY:

- To protect the elderly from the injury of fall accident events or to give an immediate assistance to the elderly after the occurrence of a fall accident event. It is a fall detection algorithm. The angles acquired by the electronic compass (e compass) and the waveform sequence of the triaxle accelerometer on the smart phone are used as the system inputs.

ADVANTAGES:

- Every day using hand held device(mobile). more comfortable.
- Better accuracy compares from existing

VI. LITERATURE SURVEY:

Title: Detecting falls with wearable sensors using machine learning techniques
Author: Ahmet TuranÖzdemir,BillurBarshan
Year: 2014

Description : Falls are a serious public health problem and possibly life threatening for people in fall risk groups. We develop an automated accident system with wearable motion sensor units fitted to the subjects' body at six different positions. Each unit comprises three tri-axial devices (accelerometer, gyroscope, and magnetometer/compass). Fourteen volunteers perform a standardized set of movements including 20 voluntary falls and 16 activities of daily living (ADLs), resulting in a large dataset with 2520 trials. To reduce the computational complexity of training and testing the classifiers, we focus on the raw data for each sensor in a 4 s time window around the point of peak total acceleration of the waist sensor, and then perform feature extraction and reduction.

Title: A Survey on Ambient-Assisted Living Tools for Older Adults
Author: ParisaRashidi and Alex Mihailidis.
Year: 2009

Description : In recent years, we have witnessed a rapid surge in assisted living technologies due to a rapidly aging society. The aging population, the increasing cost of formal health care, the caregiver burden, and the importance that the individuals place on living independently, all motivate development of innovative-assisted living technologies for safe and independent aging. In this survey, we will summarize the emergence of 'ambient-assisted living" (AAL) tools for older adults based on ambient intelligence paradigm. We will summarize the state-of-the-art AAL technologies, tools, and techniques, and we will look at current and future challenges.

VII.CONCLUSION:

Wide utilization of sensor-rich smart devices created a new attack surface namely sensor-based attacks. Accelerometer gyroscope, light, etc. Sensors can be abused to steal and leak sensitive information or malicious Apps can be triggered via sensors. Security in current smart devices lacks appropriate defense mechanisms for such sensor-based threats. In this paper, we presented 6thsense, a novel context-aware task oriented sensor-based attack detector for smart devices. We articulated problems in existing sensor management systems and different sensor-based threats for smart devices. Then, we presented the design of 6thsense to detect sensor based attacks on sensor-rich smart devices (smartwatch and smartphone) with low-performance overhead. 6thsense utilized different machine learning (ML) techniques to distinguish malicious activities from benign activities on a device. To the best of our knowledge, 6thsense is the first comprehensive context-aware security solution against sensor based threats. We evaluated 6thsense on real devices with 100 different individuals. 6thsense achieved over 97% of accuracy with different ML algorithms including Markov Chain, Naive Bayes, and LMT. We also evaluated 6thsense against three different sensor-based threats, i.e., information leakage, eavesdropping, and triggering a malware via sensors. The empirical evaluation revealed that 6thsense is highly effective and efficient at detecting sensor-based attacks while yielding minimal overhead.

VII. REFERENCES:

[1] M. Chan, E. Campo, D. Est`eve, and J.-Y. Fourniols, "Smart
homes—current features and future perspectives," Maturitas,
vol. 64, no. 2, pp. 90–97, 2009.
[2] S. Poslad, Ubiquitous computing: smart devices, environments and
interactions. John Wiley & Sons, 2011.
[3] A. K. Sikder, A. Acar, H. Aksu, A. S. Uluagac, K. Akkaya, and
M. Conti, "Iot-enabled smart lighting systems for smart cities,"in Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual. IEEE, 2018, pp. 639–645.
[4] E. Macias, A. Suarez, and J. Lloret, "Mobile sensing systems,"
Sensors, vol. 13, 2013.
[5] Z. B. Celik, L. Babun, A. K. Sikder, H. Aksu, G. Tan, P. McDaniel,
and A. S. Uluagac, "Sensitive information tracking in commodity
iot," in 27th USENIX Security Symposium (USENIX Security 18),
Baltimore, MD, 2018, pp. 1687–1704.
[6] A. Uluagac, V. Subramanian, and R. Beyah, "Sensory channel
threats to cyber physical systems: A wake-up call," in IEEE Conference
on Communications and Network Security (CNS), 2014, pp.
301–309.
[7] R. Hasan, N. Saxena, T. Haleviz, S. Zawoad, and D. Rinehart,

"Sensing-enabled channels for hard-to-detect command and control
of mobile devices," in Proceedings of the 8th ACM SIGSAC
Symposium on Information, Computer and Communications Security,
2013, pp. 469–480.
[8] T. Halevi and N. Saxena, "A closer look at keyboard acoustic
emanations: Random passwords, typing styles and decoding techniques,"
in Proceedings of the 7th ACM Symposium on Information,
Computer and Communications Security, ser. ASIACCS '12, pp. 89–
90.
[9] A. Maiti, O. Armbruster, M. Jadliwala, and J. He, "Smartwatchbased
keystroke inference attacks and context-aware protection
mechanisms," in Proceedings of the 11th ACM on Asia Conference on
Computer and Communications Security, 2016, pp. 795–806.