Surveillance of Smart Home based on Mobile alerts through Wireless Sensors

V.Parthipan
Saveetha School of Engineering
Saveetha University

N.Duraimurugan
Saveetha School of Engineering
Saveetha University

T.Rajasekaran
Saveetha School of Engineering
Saveetha University

ABSTRACT
Since it is not possible to be at home and workplace at a single time but it is important to monitor our families and most valuable possessions at home which can be made possible with pervasive technologies. In this paper, we present home alert notifications on mobiles with the help of sensors and wireless cameras so that we can feel free while away from home. A model is proposed in which sensor learns the activity of all persons entering in home and generates alert notifications on administrator's mobile when a person deviates from its normal activity. If an anonymous person comes, he is tracked every time and notifications are generated when he tries to affect any device or lock. The model has the capability to categorize persons on the basis of criteria and decide the functionalities and access available to them in the smart home. It has the facility of monitoring the devices used and generates alerts when any device starts works improperly.

Keywords
Keywords-pervasive technologies, smart devices, surveillance cameras, sensors, Home Surveillance, learning

1. INTRODUCTION
The advancement of technology influences every part of our daily life. We have started to rely heavily on technologies and always adopt those technologies which make our living much simpler and as well as advanced. So significant improvements of embedded devices and ubiquitous technology has made it possible to build a home which is smart enough to track all our activities and provide most needed facilities automatically. This brings in dependence on machines which though smart in our case, is still susceptible to failures and hence needs to be actively monitored. It is a necessity to keep track the devices as well as human activity with the purpose of making safe and secure Smart Home. For this task, we need a well and strong enough surveillance system for monitoring home. In this paper, we propose an abstract model for smart home surveillance system.

In our model, humans are categorized in four groups' namely: 1.Member 2. Guest 3.Admin 4.Anonymous. This grouping is based on criteria which also enable us to decide the functionalities and access available to them in the smart home. For example, people belonging to member category will be having access to all devices present in smart home in use mode but not in configuration mode. Member category people can't decide the privileges on access control etc. as these functionalities are given to admin. The proposed home will use latest IT technology like surveillance cameras, face recognition, sensors, automated devices, secured wireless transmission etc. To facilitate the monitoring of CNG density, we placed a sensor inside the kitchen which generates notifications when CNG density exceeds its critical level simultaneously generating commands for opening of exhaust fan and windows of kitchen. .Admin can access the home intranet system remotely via Internet which is

supported with encryption and authentication techniques such that access and alteration of commands from unauthorized person can be prevented. The model also keeps an eye on the behavior of the inhabitants of home and if any suspicious activity is seen inside home, notifications are given to the admin as well as security. In another scenario, if the admin himself is in the home with the anonymous persons performing unusual activities then reports are sent only to the security. Anonymous user's area is tracked by sensor device and information is sent to admin that unrecognized person has entered in particular area. If an unauthorized person enters into server room, messages are generated for admin and security. Our sensors communicate through agents to a centralized system which analyses those agents and based on this takes decisions and informs to admin, security department etc. Autonomous sensing replaces the work of person of tracking those data with smart sensing technology.

The remainder of paper is organized as follows. Section 2 describes related works in this area. Section 3 we give environment and assumptions. Section 4 presents an abstract model of the system. Section 5 discusses about working of model. Section 6 tells about issues arising during implementation. Finally Section 7 concludes this paper with discussion on future work.

2. RELATED WORK
Worldwide there are a several research centers that are focused on Smart homes, and some of them have a special focus on the surveillance system inside a smart home. Company like IBM has IBM Smart Surveillance System which uses the open-standards based architecture of surveillance. IBM S3[6] is a middleware which can be integrated with other surveillance systems to present several exciting features such as ability to automatically monitor a scene and manage the surveillance data, perform event based retrieval, receive real time event alerts through standard web communications and extract long term statistical patterns of movement. Sensor data from a variety of sensors is converted into Meta data in the Smart Surveillance Engines (SSEs) and transferred to the backend MILS system. MILS provide numerous query and retrieval services depending on the types of meta-data existing in the database.

Stanford University has developed an Interactive Workspace design [10] which can also be applied to smart homes to provide monitoring of different appliances equipped with i-sensors of home. When a user is away from Smart home he can track about conditions of stove, light, thermostat, alarms etc. Mesh Eye [5], smart camera mote architecture provides power and energy-efficient mechanism for surveillance deployments with the use hybrid-resolution vision system.

Microsoft has presented Multi-camera Multi-tracking [12] in Easy living project [11] in order to resolve real-life troubles in vision tracking with the use of two sets of color stereo cameras creating 3D effects.

3. ENVIRONMENT AND ASSUMPTIONS

Our Proposed Smart Home Model has been made keeping in view the following assumptions-

- Appropriate sensor devices having processing capabilities to process the appropriate data locally and send information to the server.

- Strong face detection and gait analysis technologies are used to gather data and their entries are made to database for future references.

- Enough bandwidth is available to send real time video and other information to server and administrator.

- Server has strong security to prevent unauthorized access and authentication of intruder.

4. THE PROPOSED MODEL

Our model comprises of sensor devices for temperature, gas density, smoke etc. Two types of cameras are proposed to be used. One is of low resolution and the other is of high resolution. All the data received from various sensing devices and cameras are sent to a central server which may be located inside the house or in a remote place depending on the need and size of the Smart Home. We divide processing into two parts: local processing and remote processing; local processing is done at sensor devices whereas latter one is done at the server. Internet connection of enough bandwidth to transfer real time video and other information to system and administrator is a necessity.

Our model has sensor devices distributed across the home and has cameras at each entrance and within each room. The number of cameras depends upon the location and size of the place. The sensor devices continuously sense the home and process its data locally. We define a safe band which is confined within threshold values and if the devices cross this threshold value, sensors signals to the server and send their data to it. We have one low resolution camera for processing local data and one high resolution camera which turns on when any movement occurs. The server does the main and important part of the analysis and decision-making because it's responsibility to verify messages at server before forwarding to administrator or users of the system. Database is used for storing person's data, their identification and their corresponding access rights, history of the system like- video, information and processed data, user name of members and their passwords etc. The server sends and receives command either directly via some input devices like keyboard or remotely by logging in via Internet. The server's information important to user can be sent to mobile through messages, through e-mail and optionally sends to the appropriate place according to situations (like in security staff, fire bridged etc.).

5. WORKING

Firstly, system records the admin name and their password so that only valid person can set the criteria and access the important information of the system. System monitors the persons via applying face recognition and gait analysis techniques and creates entries for the particular entrance of a person. Admin assigns the person his identification and their access privileges as mentioned above. Any unrecognized user is treated as an anonymous user and will not have any access rights. System treats him as a threat and sends messages and

camera-recorded information to admin in order of recognition of anonymous user to admin as well as system. Hence only valid person can enter inside the home. Sensors monitor the user and create an event if the user trying to use the service not assigned to them and informs to admin. Model uses robust security techniques to prevent intruder from accessing and changing the data and password of the system. The sensors inside the home are designed to learn the activities of a person and deviation from any such activity creates an event in the form of messages to the admin. This infers that now it's time to pay attention towards activities occurring around your home. And if it sees that the admin also in the home with the anonymous persons performing suspicious activities then reports to security only. Sensor devices also sense its respective area and keep track of activities which is under its area such as in the kitchen to sense CNG density and if the density increases more than critical level, the system informs the user alarming in the home and takes some appropriate steps like opening of exhaust fan, opening of window etc. If any leakage of current is found in the circuit by sensor devices then it notifies the user to take action and after sometime it cuts the power supply of that particular area.

We take particular care of devices such as refrigerator, air conditioner. Suppose refrigerator is in on state and its evaporator fan has not been in motion from 3 hours simultaneously the temperature sensor inside fridge shows increased temperature, then probability of evaporator fan of being defective can be inferred up to some extent. Attaching motion detector sensor with evaporator fan, pressure measure sensor inside compressor, temperature sensor with defrost heater and smoke detector inside refrigerator for toxic fumes will make us aware towards malfunctioning of refrigerator. Such action we can perform with air conditioners. Putting sensors with component of devices is feasible form the cost point of view because some detectors are very simple and inexpensive cost varying from $15-$25.

Camera of low resolution is on all the time and it examines the scene locally and if it finds any movement than it turns on the high resolution camera which keeps track all activities during movement and take snaps of the recorded video and by processing it locally sends important snapshots of the events to the server. The database by default keep the data in the history for only some predefined time and if admin want to keep any data for a long time it mark that data and assign time limits for that.
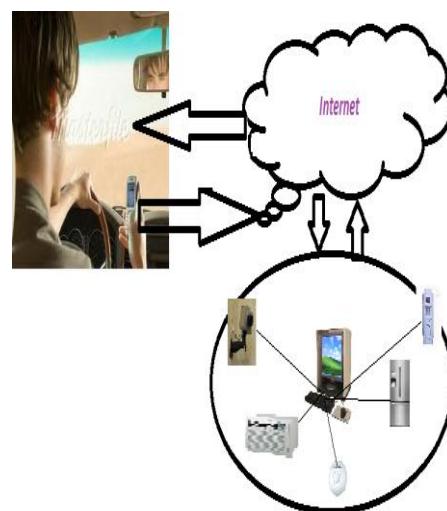

Figure 1: Smart Surveillance System

6. LIMITATIONS

Although the abstract model we proposed is well-suited for smart home but there are some limitations associated which are pointed below:

Bandwidth- Although, the model allows monitoring the home via low resolution cameras nevertheless uses high definition cameras for real time data generation, which is of big in size and requires high bandwidth. Even though we reduce it by doing computation locally. Before sending to server camera processes the data and sends only those selected snaps or clips which it finds useful.
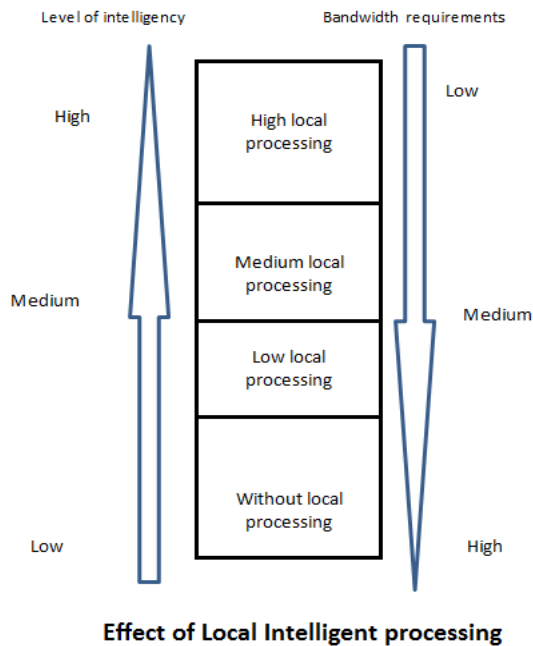

Figure 2: Bandwidth Utilization with Intelligence

Single point failure- As the server acts as the master of the whole systems so in case if it fails the whole system fails.

Security- Because system is using wireless communication for data exchange so it is prone to risks of security. Therefore, probability of hacking and damaging of system by intruder still reside up to some amount.

Lack of proper face recognition and gait analysis technique

Privacy issues - Due to privacy rule, video surveillance cameras are prevented at some places, which create drawbacks in surveillance system.

Database related issue - how much and which type of data we should have to maintain in database and how to apply some time constraints in our database.

7. CONCLUSION AND FUTURE WORK

Recent technology innovation has greatly affected the area of home surveillance. The fast growing fields like IT and Nano technology will force us to use smart and secure devices in our home for privacy as well as security. The proposed surveillance will generate huge real time data .Storing and analyzing this data in real time is a major issue and requires further work. The devices need to be intelligent and learn with the usage. The future work on this topic may include Scalability, Artificial Intelligence, distributed database, fault-tolerance and reliability. Further, we can develop the surveillance system with different modes based on user requirements for efficient energy utilization.

8. REFERENCES

[1] http://news.consumerreports.org/appliances/2012/01/new-refrigerator-featuresand-how-to-keep-food-fresh.html

[2] http://www.smarthome.com/7026/Sensaphone-Smoke-Detector-w-Battery-Backup/p.asp

[3] www.infj.ulst.ac.uk/~jcaug/introbook06.pdf

[4] *"Performance Analysis of Gait in Camera Networks"*eprints.ecs.soton.ac.uk/17033/1/paper_ACM_08.pdf

[5] Mesh Eye: *"A Hybrid-Resolution Smart Camera Mote for Applications in Distributed Intelligent Surveillance"* Stephan Hengstler, Daniel Prashanth, Sufen Fong, and HamidAghajan, Stanford university

[6] IBM Smart Surveillance System (S3):*"Event Based Video Surveillance System with an Open and Extensible Framework"*, Ying-li Tian, Lisa Brown, ArunHampapur, Max Lu , Andrew Senior and Chiao-feShu,IBM T.J Watson Research Centre.

[7] *"Prototype Model for Real Time Home Surveillance System over the Internet"* RathikaRajaravivarma, New York City College of Technology

[8] *"Survey and Analysis of Multimodal Sensor Planning and Integration for Wide Area Surveillance"* Besma R. Abidi, Nash R. Aragam, Yi Yao, and Mongi A. Abidi, The University of Tennessee

[9] http://www.smarthome.com/_/index.aspx

[10] hci.stanford.edu/cstr/reports/2004-05.pdf

[11] http://research.microsoft.com/en-us/um/people/jckrumm/Publications%202000/huc2k-final.pdf

[12] http://research.microsoft.com/apps/pubs/default.aspx?id=68612

[13] http://www.magarchive.tcu.edu/articles/2003-02-AC.asp?issueid=200302

[14] http://www.geindustrial.com/cwc/electrical_homepage.htm