Smart Home With CyberSecurity Features

Without Sensors and web-camera Technology

Abdur Rafay
Computing and information Technology
University of Gujrat
Gujrat, Pakistan
14241556-057@uog.edu.pk

Muhammad Waqas
Computing and information Technology
University of Gujrat
Gujrat, Pakistan
14241556-056@uog.edu.pk

Hammad Sami
Computing and information Technology
University of Gujrat
Gujrat, Pakistan
14241556-040@uog.edu.pk

Abstract:

Nowadays, security threats are becoming important problem in the world. Everyone in this world want to keep an aye on his house due to threats and risk of theft and robbery, danger of leaking raw gas, and also requires safety from fire, at the same time they want to save energy, and also want to keep an eye on their house if there are elders or disabled person in the house.

This system sends the images and the threat messages to warn the people about the danger in SMS or MMS form. This system monitors the irregular activities and functions with the help of sensors and most importantly with the web camera and then performs necessary actions to save assets and warn the authorized person to take serious steps.

Introduction:

Smart home is usually known by automatic home or AI(artificial intelligent)home as well and security system keeps update to owner of that house while he is far away from home or out of country.

Security of a house has become an important issue now a days[1-3]. it is important because of danger of Intruder, Theft, Robbery, Raw gas leaking, and Fire and these are the most important aspects or features of a home security system as well[4-10]. The difference between traditional and modern home security systems is that, in traditional home security system, the system uses sensors, like IR(Infrared) is used to detect stranger and intruder and generally used at doors and windows, for temperature monitoring the LM35 is used as temperature sensor, light dependent resistor(LDR) is used to sense the amount of light in a room. But all these sensors uses a lot of resources and money so are they suitable for us.

This security system also uses the GSM technology to send SMS to owner's number, relays to make a connection between devices and buzzers to make sound to gain possible help from around and gives the signals in terms of alarm and also send the SMS to owner's mobile. But in advanced or modern security home system, the security system takes necessary actions like sending message to defined cell no in the system, and could also call to nearest police or help center as well. It includes the web camera installed in the house used by the special software and can communicate with internet facility and can send email to desired email ID to warn the owner about danger and risk, It also uses the above mentioned sensors, relays to connect different devices and buzzers to make sound as well.

the security system uses the web camera and special sensors to catch the unnecessary motion and unwanted actions[9-14]. special sensors can include the heat sensors, fire sensors, and humidity sensors etc. when security system monitor the extraordinary activities then the system could take special actions to eliminate the risk and avoid from the loss. But our security system model uses no additional user resources like cameras IR sensors etc. because our model converts a simple smart home into a complete secure house without the additional use of resources.

Background:

As our main focus is on the security factor of the smart houses so we are taking into account the best security systems used in the smart houses Vivint smart home, Front point Home Security System, Protect America Home Security etc. before analyzing these smart home security systems we will analyze the factors and resources uses in these security measures so far.

IFTTT support:

IFTTT is a web based service in which people can create chains of simple conditional statements also known as applets which can be triggered by simple changes in which user can create his own conditions on which its security measures depend.

Canary system:

The Canary supports the idea of connecting all of your smart devices together for an approach of making one security system that can do a lot. It's very easy to set up and then will monitor your house, watch for intruders and keep the owner updated[6, 7, 15].

Cellular Backup:

Mobiles are important part of security systems of smart house because owner is updated on his house condition simultaneously so cellular backup is of most importance so the owner can be updated correctly.

Power Outage Backup:

Power outage is major concern so in smart houses there should be a secondary power source so the security system keeps working when there is no power and it should not fail in power outage.

Environmental Sensors:

all the security systems use thermal, IR and motion sensors to make sure that the house is secure and to avoid the theft.

After describing the main factors and tech uses in smart houses lets discuss how we can secure the house on 2^{nd} grade without any expensive sensors or security measures.

Procedure:

To develop a system which is cost effective and efficient and provide a secure environment we developed a model which does not require new and state of the art sensors such IR motion etc. The only thing it requires is any smart home module which has simple WIFI and GPRS connecters so the user can get the information about his house in real life using his phone or PDA using Short Message Service (SMS) which would require a connection to the internet. All home appliances like LED lights and fans are connected to the module. The only thing we require is a software integration in the smart home module.it would use a Boolean algorithm which would record the state of all the appliances connected to the smart house module.

Software design:

In the proposed system programming is done in 'JAVA' language and to configure it extreme burner is used. The algorithm maintains a virtual lockdown status of the house on change of the status of the lockdown. The software notifies the owner of

that situation and guides the owner on what to do and how to deal with the situation. The algorithm has a function which changes the lock down status of house.

Pseudocode

If

lockdown status is equal to zero

Do not invoke lockdown (function)

Else

Invoke lockdown (function)

Lock down function:

initialize appliances [] with current status

if appliances value changes

notify owner

initialize action to zero

get owner reply

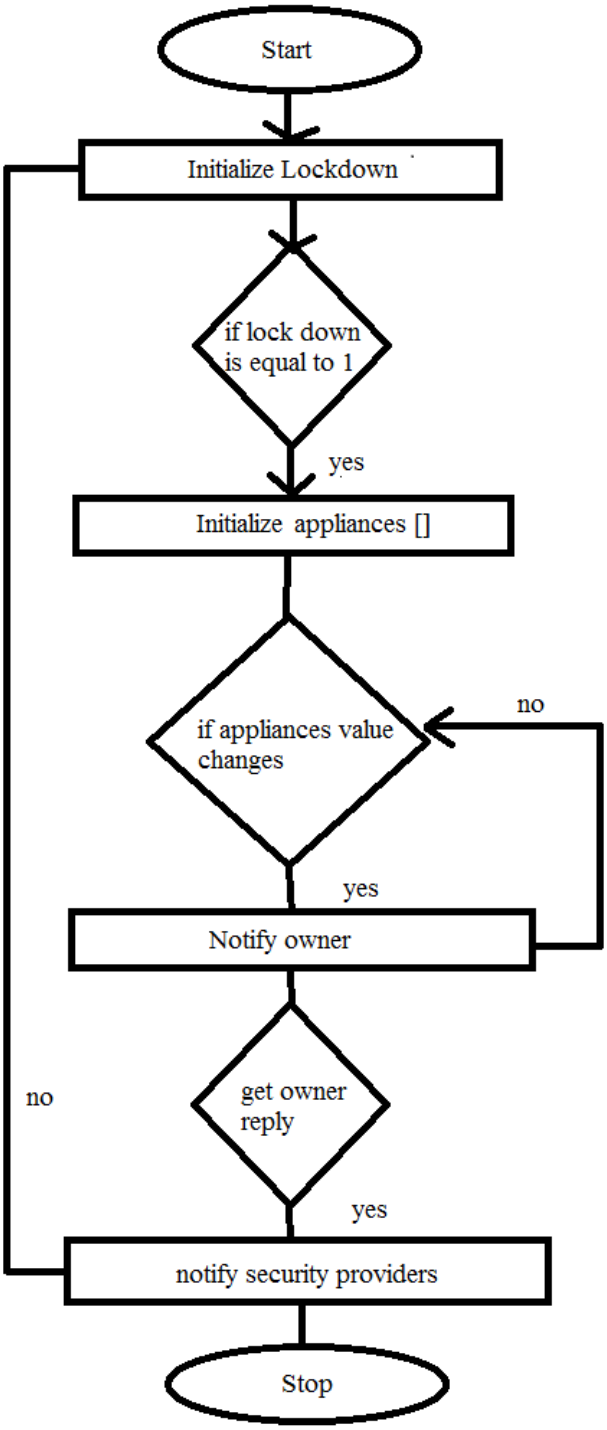
if action value is equal to 1

notify security companies

else break

else continue monitoring

If the user leaves the house the lockdown function invokes. The user puts the house on the lockdown state using his phone and the function saves the current state of all the home appliances and in case of intruders attack the states of the appliances changes and the system then notifies the relevant users about the change in state of the house in his absence and asks the user about the seriousness of the situation if the user ignores the request the system then maintains its current state otherwise the system notifies the authority to counter the intruder.



Flow Chart of the System

Hardware Design:

The hardware of the system uses sim548c (GSM module) and the smart home module in system programmer that relays to control the appliances. The outputs of all the sensors are connected to the smart house module. A SIM548C based quad band GSM module which supports GPS technology for satellite navigation is used. It provides GPRS multi-slot class10 / class8 capabilities and supports GPRS coding schemes

Achievement:

By implementing the system the cost of the system decrease exponentially because the system does not require additional sensors to keep the house secure and if the model is used while using the additional security measures it will increase the security factor of the property.

Results:

This system for smart home is very simple, cost effective, and easy to use as well. Mostly this system uses SMS technology to warn the authorized person about the danger so it is cheaper in terms of cost as it does not cost data charges because of MMS but still there is a option to use the MMS service.

This combination of hardware and software is very reliable, Convenient, and easy to use but still there is a chance to not get the warning message because of poor telecom services in some areas in the world or sometimes elders find it difficult to use the technology or not properly able to read or understand the message from cell phone.

Acknowledgement:

The authors have to say thanks and acknowledge to our honorable and respected professor Mr. Nauman Mazhar from IT Department, University of Gujrat, for their support and help and most importantly encourage us to write this research paper and helped a lot to complete this task.

Conclusion:

This research paper gave the idea about hardware design, software design, flow chart of the system's working and execution and also gives idea through pseudocode that how situation will be handle if there is something wrong and dangerous. This system has been tested on the smart home model and it can also be tested on actual and real home as if we got funds.

There is flexibility in the system that users can get information and output both on PC and mobile via SMS and MMS technology as well. but it will be more convenient and easy for users to get the warning messages on cell phones as it will be easier for them to monitor their houses whether they are in any corner of the world.

References:

[1] M. Du, Z. Chen, C. Liu, R. Oak, and D. Song, "Lifelong anomaly detection through unlearning," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1283-1297.

[2] H. Jain, R. Oak, and J. Bansal, "Towards Developing a Secure and Robust Solution for E-Voting using Blockchain," in *2019 International Conference on Nascent Technologies in Engineering (ICNTE)*, 2019: IEEE, pp. 1-6.

[3] K. S. Jhala, R. Oak, and M. Khare, "Smart collaboration mechanism using blockchain technology," in *2018 5th IEEE International Conference on Cyber*

Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2018: IEEE, pp. 117-121.

[4] M. Khare and R. Oak, "Real-Time distributed denial-of-service (DDoS) attack detection using decision trees for server performance maintenance," in *Performance Management of Integrated Systems and its Applications in Software Engineering*: Springer, 2020, pp. 1-9.

[5] J. C. Newman and R. Oak, "Artificial Intelligence: Ethics in Practice," *login Usenix Mag.,* vol. 45, no. 1, 2020.

[6] R. Oak, "A study of digital image segmentation techniques," *Int. J. Eng. Comput. Sci,* vol. 5, no. 12, pp. 19779-19783, 2016.

[7] R. Oak, "Extractive techniques for automatic document summarization: a survey," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 4, no. 3, pp. 4158-4164, 2016.

[8] R. Oak and M. Khare, "A novel architecture for continuous authentication using behavioural biometrics," in *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, 2017: IEEE, pp. 767-771.

[9] R. Oak, M. Khare, A. Gogate, and G. Vipra, "Dynamic Forms UI: Flexible and Portable Tool for easy UI Design," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018: IEEE, pp. 1926-1931.

[10] R. Oak, M. Du, D. Yan, H. Takawale, and I. Amit, "Malware detection on highly imbalanced data through sequence modeling," in *Proceedings of the 12th ACM Workshop on artificial intelligence and security*, 2019, pp. 37-48.

[11] R. Oak, "Poster: Adversarial Examples for Hate Speech Classifiers," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2621-2623.

[12] R. Oak, C. Rahalkar, and D. Gujar, "Poster: Using generative adversarial networks for secure pseudorandom number generation," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2597-2599.

[13] R. Oak, "The Fault in the Stars: Understanding the Underground Market of Amazon Reviews," *arXiv preprint arXiv:2102.04217,* 2021.

[14] V. Sehwag, R. Oak, M. Chiang, and P. Mittal, "Time for a background check! uncovering the impact of background features on deep neural networks," *arXiv preprint arXiv:2006.14077,* 2020.

[15] R. Oak, "A literature survey on authentication using Behavioural biometric techniques," *Intelligent Computing and Information and Communication,* pp. 173-181, 2018.