International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Smart Homes

D.Ganesh kumar
Computer Science
Bhavans Vivekananda College
Hyderabad

B Bala Krishna
Computer Science
Bhavans Vivekananda College
Hyderabad

K Sai Praneeth
Computer Science
Bhavans Vivekananda College
Hyderabad

Abstract: A smart home is a new one that is equipped with special structured wiring to enable occupants to remotely control or program an array of automated home electronic devices by entering a single command. The home network encompasses communications, entertainment, security, convenience, and information systems. A technology known as Power line Carrier Systems (PCS) is used to send coded signals along a home's existing electric wiring to programmable switches, or outlets.
Problems with smart home: Hacking Connected Thermostats, Who's really Watching Your Smart TV, Compromised Security Systems, Eavesdropping on Communication Systems, Changing Lighting Systems. Internet like IPv6,etc.

I. INTRODUCTION *(SMART HOME)*

Early home automation or smart homes began with labor-saving machines. Self-contained electric or gas power home appliances became viable in the 1900's with the introduction electric power distribution and led to the introduction of washing machine (1904), water heaters (1889), and many more house appliances.

In 1975, the first home automation network technology "X10" was developed. It is mainly based on communication protocol that was used for electronic devices. It uses electric wiring for transferring signaling and control, where the signals uses radio frequency bursts of digital data, and remains the most widely used. By 1978, X10 products added 16 channel command console, a lamp module, and an appliance module. Soon after came the wall switch module and the first X10 timer. The word "*domotics*" is a contraction of the Latin word for a home (*domus*) and the word robotics.

Types of Generation in Smart Homes

There are mainly 3 Generation

- **First generation(Wireless Technology and proxy server approach)**
- **Second generation(Artificial Intelligence control the Electrical devices)**
- **Third generation(Robot buddy who can interact with human being)**

1. **Wireless Technology and proxy server approach:** the first generation smart home technology use wireless communication like Bluetooth,etc. to interact and monitor the electrical devices.But,there was a problem that more than one Bluetooth interaction Leeds to error.So,A local Proxy server was created that creates communication trough inter

   E.g. Zigbee automation.

2. **Artificial Intelligence control the Electrical devices:** the second generation was a moderate development of the traditional technique by using the features from the traditional technique and taking help of AI(artificial intelligence) and multi agent system, **SHE(smart home environment)** was developed. This system gives a primary knowledge to the devices of learn understand and communicate with each other through internet.
   E.g. Amazon Echo.

3. **Robot buddy who can interact with human being:** The more advance development of AI is the robot buddy. That is a robot that has primary knowledge to do things and communicate with is users by recognizing the voices and following the instructions like a robot name buggy. It is called and by the voice reorganization it follows the command like to on A/c or any other electrical instrument and of it on the owner/instructor leaves.
   E.g. Robot Rovio, Roomba.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Applications and Technologies

- **Heating, ventilation, Air condition (HVAC):** it is possible to have remote control of all home energy monitors over the internet incorporating a simple and friendly user interface.

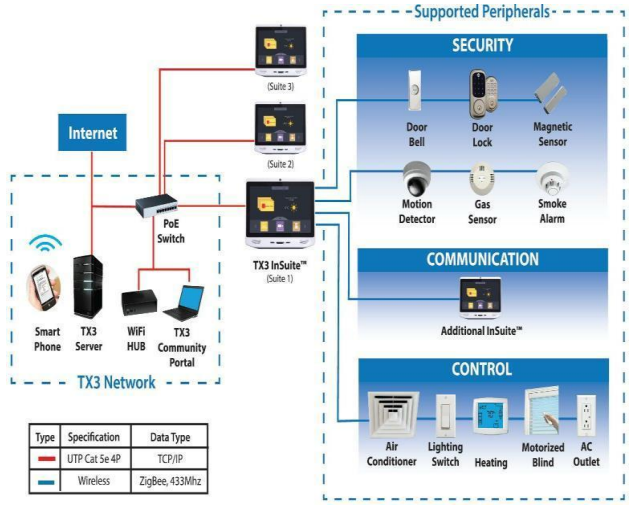
  Lighting control system

  Occupancy-aware control system: it is possible to sense the occupancy of the home using smart meters and environmental sensors like CO2 sensors, which can be integrated into the building automation system to trigger automatic responses for energy efficiency and building comfort applications.

- Appliance control and integration with the smart grid and a smart meter, taking advantage, for instance, of high solar panel output in the middle of the day to run washing machines.

- **Security:** a household security system integrated with a home automation system can provide additional services such as remote surveillance of security cameras over the Internet, or central locking of all perimeter doors and windows.

- Leak detection, smoke and CO detectors.



Limitations/Defects of Smart home using WIFI

The main disadvantage of the smart home is that it runs completely on the internet. The **Directed Denial of Service (DDoS) attack,** the resent **Ransomware** that brought the Internet and other communication system to its knees. That's likely to become increasingly commonplace in a technology-dependent world, experts say. The stakes are mounting as "smart home" devices — connected by increasingly ubiquitous Internet of Things technology and designed to help consumers run their homes with ease — now come with a distinct risk. They are being transformed into drones for security breaches.

"Security has not been a prime focus on many devices and organizations that put these out helter-skelter. In many cases they're not adjusting to security concerns," **Leonard Klein rock**. "So it's not a surprise this [cyber attack] happened and it hasn't been taken seriously. There's no oversight in general."

According to **Klein rock**, that's a major concern in the context of seemingly relentless cyber warfare. A big problem is that most consumers use default passwords on these appliances that can easily be hacked.

Not only that the resent attack of the Ransomware, was also a wakeup call to all the people about the security issues in the internet as the attack was done by the internet and took the value information of many countries communication.

The poor security in Internet of Things products -- including IP connected security systems, connected climate control and energy meters, smart video conferencing systems, connected printers, VoIP phones, smart fridges, and even smart light bulbs -- pose an inherent risk to the security of private information.

The researchers say smart video conferencing systems, connected printers, and VoIP phones all represent easy IoT-connected targets which provide a gateway for hackers to snoop on the targeted person private information.

The resent research says that ” Not only do these devices pose significant risks due to a lack of rudimentary security, but many were found to be operating with out-of-date firmware. These vulnerabilities can be easily exploited to plant backdoors and launch automated IoT botnet DDoS attacks”. The best example in resent day is **Ransomware.**

Few common ways those attackers are hijacking IoT devices:

1. **Mass Vulnerability Probing:**“Internet-connected devices are being churned out of factories and infected by malware, or malicious code.

2. **Exploiting Universal Plug-and-Play (**uPNP**):** One of the ways that attackers breach devices is through their uPNP, a technology that provides an instant, seamless connection to network-enabled devices. Devices, such as video cameras, use uPNP to talk to your router and accept outside connections. “This makes it easier to access them from the internet, but it also exposes your devices to the rest of the world.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

3. **Intercepting the Cellular Network:** A number of IoT devices rely on cellular connections to function instead of WiFi. But while connecting a device to the internet can open the door to attackers, using a cellular network instead isn't a completely secure option either.

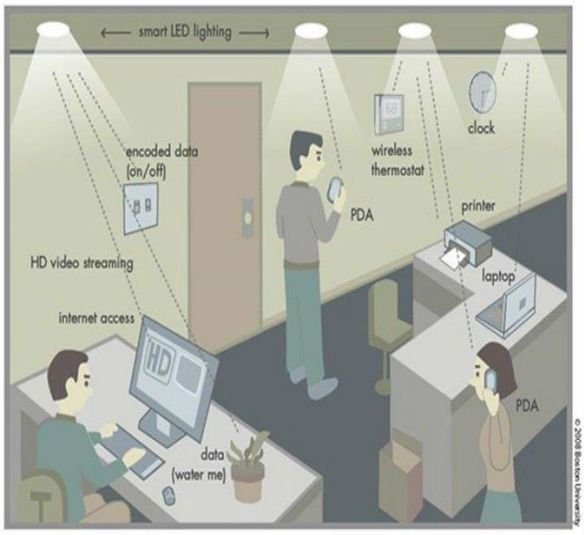
Proposed Solution

As the main Dis-Advantage of the Wifi technology is that it could be hacked by a remote server while using internet .So, to avoid that we use Lifi technology which cannot be hacked through a remote server. Since, Lifi technology uses the light for data transmission which cannot penetrate through the physical barriers so it is difficult for the unauthorized users to detect and access the network, so hacking can be prevented through remote servers.

What is Lifi?

Lifi is transmission of data through illumination by taking the fiber out of fiber optics by sending data through a LED light bulb that varies in intensity faster than the human eye can follow. Lifi is the term some have used to label the fast and cheap wireless-communication system, which is the optical version of Wifi.

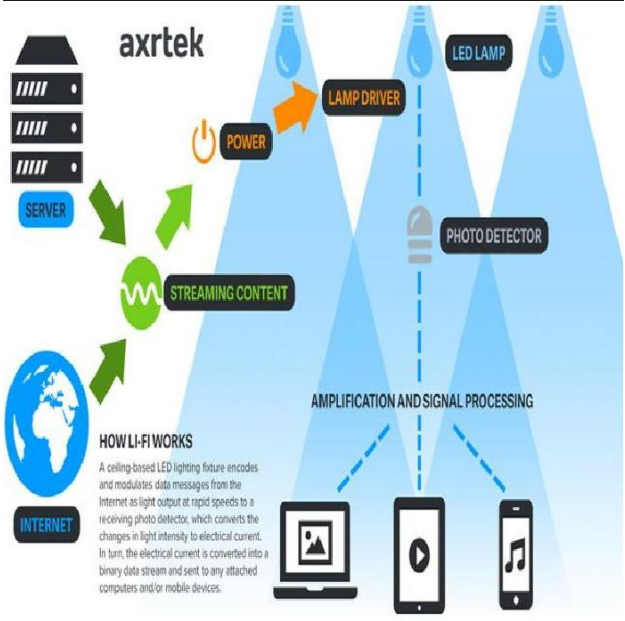
4. "At the heart of this technology is a new generation of high brightness light-emitting diodes", says Harald Haas about Lifi.



Li-Fi Vs Wi-Fi

Features	LiFi	WiFi
Full form	Light fidelity	Wireless fidelity
Operation	It transmits data using light with the help of LED bulbs	It transmits data using radio waves with the help of routers
Interference	It doesn't have any interference issues	Interference can occur through the other routers
Merits	It can travel through high density region like water,etc	It can travel through low density region only
Security	It doesn't pass through walls so secure data transfer is possible	As it pass through so additional security is needed
Data transfer speed	About 1Gbps	Wlan-11n can offer 150mbps,1-2gbps can be achieved through Giga-IR
Technology	Present IrDA	WLAN 802.11a/b/g/n/ad /ac
Data density	Works in high density environment	Works in less density due to interference issues
Coverage distance	About 10meters	About 32 meters
System components	Lamp drivers, LED bulbs	Required routers and subscribers like Pc,laptop,etc

Lifi Technology Design



Drawbacks

- As every technology has ups and downs here the lifi technology also has some downs (drawbacks).
- As we know Home automation works with sensors it controls the lighting of the house. For example when a person enters the room lights automatically gets ON and when he walks out of the room lights gets OFF.
- Lifi technology is associated with the LEDS, when a person walks out of the room the lights gets off automatically it effects on the connectivity as lifi works with visible light. Data transmission is interrupted
- Individual infrastructure is required for both lighting of the house and for lifi technology, which may cost.

Conclusion

- In the above presentation we have seen the advantages & disadvantages of smart home technology using Wifi technology.
- As the major drawback of the WIFI technology is it can be easily hacked through the main server that is connected to the devices.
- Our proposed system is using LIFI technology by replacing WIFI technology
- Lifi technology uses light emitting diodes for data transmission as light cannot pass through the physical barriers its range is fixed .It is difficult for the Unauthorized users to detect the signals so there is a less chance of being hacked.
- Lifi technology is cheaper than Wifi technology.
- It reduces the cost of the installation as it comes along with the LED's.
- Hence, Smart home devices using Lifi technology is better than Wifi technology as it provides high security.

References

[1] https://en.wikipedia.org/wiki/Home_automation

[2]http://www.mirror.co.uk/tech/smart-home- devices-could-criminals-10361249

[3] https://hologram.io/4-ways-cyber-attackers-may-be-hacking-your-iot-devices-right-now/?_e_pi_=7%2CPAGE_ID10%2C5270622325

[4]https://www.quora.com/What-is-the- difference-between-lifi-and-wifi

[5]https://en.wikipedia.org/wiki/Li-Fi

[6]https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwi-tIHTyL3VAhXCp48KHfcWDDsQFgg3MAM&

url=https%3A%2F%2Fwww.techopedia.com%2F7%2F31772%2Ftechnology-trends%2Fwhat-are-the-advantages-and-disadvantages-of-li-fi-technology&usg=AFQjCNG8N7HARhMlczs68VWnzzy7rnO1UA