Application of Artificial Intelligence and Internet of Things in Home Automation

Mishra Jyoti Prakash[1]*, Mishra Sambit Kumar[2]

[1]Gandhi Institute for Education and Technology, Baniatangi
E-mail : jpmishra@gietbbsr.com

[2]Gandhi Institute for Education and Technology, Baniatangi
E-mail : sambitmishra@gietbbsr.com

*Corresponding Author

Abstract

The term home automation offers remote and timer control of systems and embedded devices such as light, heating, ventilation, entertainment systems, appliances, etc., to improve comfort, convenience, energy efficiency, and security. However, the element of autonomous behaviour is lacking. So the technology associated with home automation builds on the progressing maturity of various areas and the Internet of Things evolution, adding artificial intelligence to the home automation field. The primary concept is based on distributed multi-agent architectures to overcome technological challenges. In particular, it is intended to include the basic mechanism to adapt and distribute the artificial intelligence to match the distributed system architecture in home automation. Applying the distributed architecture, a smart multi agent object may be thought of to support the artificial intelligence framework and to focus on the embedded resources, the sensor frameworks, and the employed algorithms.

Keywords: Control systems, Embedded system, Distributed system, Multi agent, Sensor, Actuator, Artificial intelligence

1. Introduction

Internet of Things is defined as "An open and comprehensive network of intelligent objects that have the capacity to auto–organize, share information, data and resources, reacting and acting in face situations and changes in the environment". Internet of Things is one of the last advances in Information and Communication Technologies, providing global connectivity and management of sensors, devices, users and information. The various devices communicate intelligently with one another to execute daily operations. There is minimal human intervention for the operation of devices. Every device is connected to every other device, communication with one another, transferring data, retrieving data and intelligently responding, triggering actions. The successful implementation of the IoT involves consideration of a huge number of aspects. These involve the technology used for communication, various communication protocols which form the backbone of the IoT, standards to be used for communication, hardware and embedded devices used to build the hardware, the software, operating system that is compatible with hardware and the protocols being used.

Smart Things are a group of devices which can be monitored and controlled via a hub device (central processors) and web services and Smart Things users may also be able to control and automate today's additions directly through the Smart Things applications. The Smart Things concept has four logical architectural layers, i.e. to connect to the Smart Things Hub or in some cases directly to the Cloud, to act as a gateway for getting events and messages to or from the Cloud, to provide the abstraction and intelligence layers as well as the web services that support the presentation layer and to provide the presentation layer for smart things in the form of mobile applications. Smart Things are autonomous physical or digital objects augmented with sensing, processing, acting and network capabilities and place the world of linked things at the fingertips. These are more intelligent, convenient, secure, safe and efficient as well as easy to connect the things in the physical world to the internet for automate, monitor, control. It is possible by different embedded Internet of Things technologies like RFID, EPC, barcode, IPv4 / IPv6, sensors, actuators, GIS, GPS, Wi-Fi, Bluetooth, ZigBee, NFC, ambient intelligence.

2. Review of Literature

Normann, A et al.[1] in their work has focused on hybrid imagination approach that uses the external changing conditions as an empowerment that supports the understanding of an experimenting approach. It means that the process of exploring, researching and experimenting should adapt to the changing external conditions in the form of adjusting processes and methods used, planning, and decisions. In this work these adjustments have been done based on the present knowledge level, i.e., as the research progresses more knowledge is provided, and this new knowledge then guides the adjustments for the future processes and methods.

Wang, S et al.[2] in their work have focused on performance based, service based and system based definition. The performance based definition is used to express different kind of performances in a building. The services based definition is associated with building with the service functions of communication, office automation and building automation. The system based definition provides building automation, office automation and communication network systems, and an optimal composition integrates the structure, system, service and management, providing the building with high efficiency, comfort, convenience and safety to user.

Xiaojuan, Z et al.[3] in their work have focused on a home automation gateway that controls home automation devices and take care of illegal access or intrusion from the outside world.

Mingyi, M et al.[4] in their work have introduced a home automation management system that combines devices and the internet by using a microcontroller.

Basil Hamed et al.[5] in their work have focused to design and implement a control and monitor system for smart house. Smart house system consists of many systems that controlled by LabVIEW software as the main controlling system in this paper. Also, the smart house system was supported by remote control system as a sub controlling system.

Basma M. et al.[6] in their work have proposed a new design for the smart home using the wireless sensor network and the biometric technologies. It employs the biometric in the authentication for home entrance which enhances home security as well as easiness of home entering process. The structure of the system is described and the incorporated communications are analyzed, also estimation for the whole system cost is given which is something lacking in a lot of other smart home designs offers. It is designed to be capable of incorporating in a building automation system and it can be applied to offices, clinics, and other places.

C. Dixon et al.[7] in their work have discussed about architectural approach for IoT. The underlying platform for IoT is much more complicated than for smartphones. Nevertheless, if IoT is based on an underlying sensor and actuator network that acts as a utility similar to electricity and water, then, different IoT applications can be installed on this utility. While each application must solve its own problems, the sharing of a sensing and actuation utility across multiple simultaneously running applications can result in many systems-of-systems interference problems, especially with the actuators.

J. Deng et al.[8] in their work have discussed about the security problem, as transient and permanent random failures are commonplace and failures are vulnerabilities that can be exploited by attackers. However, the considerable redundancy that is available creates potential for designing applications to continue to provide their specified services even in the face of failures. To meet realistic system requirements that derive from long lived and unattended operation, IoT applications must be able to continue to operate satisfactorily in the presence of, and to recover effectively from security attacks.

ISSN: 2321-8363
Impact Factor: 5.515

S. Ravi et al.[9] in their work have focused about challenges associated with IoT. Ideally, for a quick response, given the real-time nature of many IoTs, the detection, countermeasures and repairs must run in real-time as part of a runtime self-healing architecture. Sometimes, healing requires re-programming, e.g., when an unanticipated attack occurs. In these cases, healing instructions need to be securely (with authentication and attestation) delivered to the appropriate nodes and then the node's running programs need to be amended by the runtime architecture.

S. Munir et al.[10] in their work have focused on explicitly incorporating human-in-the-loop models for driving which can improve safety, and using models of activities of daily living in home health care can improve medical conditions of the elderly and keep them safe. Although having humans in the loop has its advantage, modeling human behaviors is extremely challenging due to the complex physiological, psychological and behavioral aspect of human beings.

TRUSTe et al.[11] highlighted the fact that privacy concerns could be a significant barrier to the growth of IoT. According to the TRSUTe survey, about 60% of internet users have basic privacy awareness of IoT and they know that smart devices, such as smart TVs, fitness devices, and in-car navigation systems could collect personal activities data. Moreover, 85% of the Internet users would like to understand more about data collection.

Fortinet et al. [12] conducted a survey on the consumer interest towards the IoT marketplace focusing on the adaptation of the IoT devices by 1,801 homeowners. The survey was administered in Australia, China, France, Germany, India, Italy, Malaysia, South Africa, Thailand, United Kingdom, and the US. According to the survey, 61% of the homeowners agreed that the connected home is 'extremely likely' to become a reality in the next five years. At the same time, 68% of the respondents were 'extremely' or 'somewhat' concerned about the exposure of personal data. Around 57% of the respondents have considered privacy as an important issue in the IoT, and they currently do not understand or trust how the data collected though their IoT device would be used. According to Fortinet, 67% of the respondents consider data privacy as an extremely sensitive issue.

H. Gross et al.[13]in their work have used IPsec and TLS to provide authentication and privacy, but these methods are computationally expensive and may thus be inappropriate for many resource-limited IoT devices. Also a privacy management method is proposed that measures the risk of disclosing data to others, however, in many circumstances, the perceived benefit of IoT services outweigh the risk of privacy loss. There is thus a need for privacy-aware sharing of IoT data without sacrificing the privacy of users. In summary, these and several other prior works have yet to address the aforementioned challenges in ensuring security and privacy for IoT in a comprehensive manner.

M. Maroti et al.[14] in their work have discussed about application of many IoT applications based on a deployed sensing, actuation, and communication platform (connecting a network of things). In these deployments it is common for the devices to know their locations, have synchronized clocks, know their neighbor devices when cooperating, and have a coherent set of parameter settings such as consistent sleep/wake-up schedules, appropriate power levels for communication, and pair-wise security keys. However, over time these conditions can deteriorate. The most common (and simple) example of this deterioration problem is with clock synchronization.

K. Tsui et al.[15] in their work have focused on supervisory control in which involvement of humans takes place in two ways. In one case, the process runs autonomously. Humans intervene with the control algorithm when it is necessary typically by adjusting set points. These control problems are well understood. In the second case, the behaviors of a human are observed, e.g., eating behaviors, and interventions are controlled to improve their life. In the third case, the process accepts a command, carries out the command autonomously, reports the results and waits for further commands to be received from the human. For example, human-in-the-loop control is used in a wheelchair-mounted robotic arm to retrieve an object from a shelf. In this feedback control system, human provides input via a touch screen or joystick which is analyzed by a vision processing system to position the robotic arm to retrieve the object. In this application, a human directly controls the controller of the feedback control system and guides it to take appropriate action.

R. Acharya et al.[16] in their work have discussed that, IoT relies heavily on wireless networks which are known to be vulnerable to all type of intrusions including unauthorized router access, faulty configurations, jamming, man-inthe-middle attacks, interference, spoofing, Denial of Service attacks, brute-force attacks, traffic injections, etc.

D. Uckelmann et al.[17] in their work have discussed that there should exist different security levels since the requirements are not the same between devices. User privacy and integrity can also be endangered from the lack of data confidentiality and integrity. Unauthorized access of sensor data could interfere with the proper functioning of the system, as well as unauthorized access and control.

As discussed in K. on Security et al.[18], security issues of IoT devices occur in different instances which include technological, ethical and privacy concerns. In October 2016, the massive Distributed Denial of Service (DDoS) attack on Dyn - a company that controls much of the Internets domain name system (DNS) infrastructure - by a botnet army of IoT infected devices, has turned on the alarms on the consequences that faulty IoT protections and poor standards can motivate which accentuates the need for additional research on the IoT security domain.

O. Vermesan et al.[19] in their work have distinguished issues and challenges that the IoT community needs to address in order to prevent privacy violation. It includes self-aware behaviour of interconnected devices, data integrity, authentication, heterogeneity tolerance, efficient encryption techniques, secure cloud computing, data ownership & governance, as well as policy implementation and management.

R. Roman et al.[20] in their work have proposed solutions to the Iot privacy problems, the first one is to provide "privacy by design" which advocates for users to have the tools to dynamically control the data collected, stored and shared, user's request should be correlated and evaluated to existing policies in order to make a decision.

L. Tan et al.[21] in their work have discussed that technological solutions are not enough to address the current privacy issues and calls for the consideration of economical and socio-ethic aspects of the IoT environment.

S. Babar et al.[22] in their work have proposed the use of lightweight cryptographic algorithms so that the resource-limited IoT devices, especially for processing and
storage capabilities, can provide data protection and, therefore, confidentiality. In this regard, they have thought for Datagram Transport Layer Security (DTLS) which may be used as a solution to confidentiality problems by providing end-to-end security for the application layer.

S. H. Hong et al.[23] in their work have proposed smart home energy management system and suggested idea to rationale most of the home appliances to manageable loads category. This idea was established and supported, since manageable appliances, e.g. washing machine, refrigerator, air conditioner, etc. have a comparatively higher energy consumption than non-manageable appliances e.g. television and lights. Further, a larger portion of efforts were aimed to manage energy consumption by shifting electrical loads of household appliances.

S. Rani et al.[24] in their work have discussed on services based on advanced solutions along with high data rate internet service. It is observed that providing high data rate internet service increases the chance of interference in a smart home environment. Therefore, an efficient communication model may be proposed to lessen the occurrence of interference due to the heterogeneous technologies present in a smart home.

3. The necessity of home automation

The necessity of home automation is to make life easier for its residents by controlling essential functions such as light, heat, ventilation, entertainment systems, appliances etc. to improve comfort, convenience, energy efficiency, and security. But it requires the parameters to be pre-programmed by the users, i.e., it cannot be done automatically. The home automation concept is not autonomous in any way. It is simply remote controlled by the users to do timer based or pre-programmed functions that can be either simple or more complex.

Modern Home Automation homes of today are wired by power lines, TV outlets and they are equipped with Internet that is delivered wireless or by wire. So, these connections make it possible to remote control domestic activities and devices such as houseplants, entertainment systems, pet feeding, yard watering, and control different kinds of domestic robots like vacuum cleaners. Thus, it is possible to remote control these from either a near or a more distant place using a personal computer or a modern smart phone.

4. Artificial intelligence in smart homes

Commonly the term smart home creates associations to a home that are able to think on its own and act intelligently by using some kind of AI. The services and devices offered today by smart homes are much closer to what are offered by the home automation area. So, today real smart homes are not available at a commercial level, they primarily exist at a laboratory level e.g., as living labs. From a more theoretical point of view the research area dealing with adaptive AI in smart homes is in its infancy. While discussing an adaptive scenario-based reasoning system, it is based on simple user descriptions and a lightweight learning methodology. It is only partly adaptive and uses a non-portable simplified user profile management system. From the given scenario, it may be assumed that the partly intelligent smart home area may play an important role in the IoT technologies.

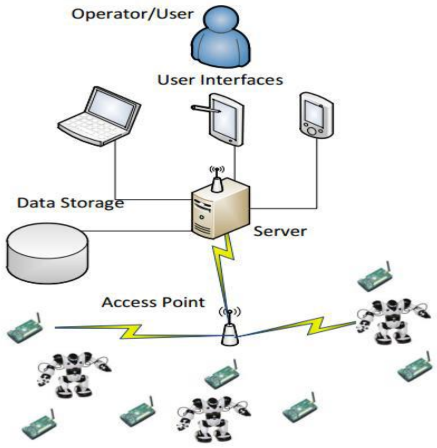

Figure 4.1 (Wireless sensor and actuator network)

The figure 4.1 represents the wireless sensor and actuator network associated to smart home. In the process of moving from automated homes to real smart homes the availability of cheaper faster Internet connections and cloud services may cause a gradual replacement of centralized automated home servers with cloud based solutions.

ISSN: 2321-8363
Impact Factor: 5.515

Centralized smart homes use architectures with a single home automation server connected to the Internet. This server receives all sensor events and it runs the AI algorithms. Based on sensor inputs and predictions it schedules services to the user. In this context the main difference between the centralized and the distributed concept is in the underlying network that supports the devices with communication capabilities.

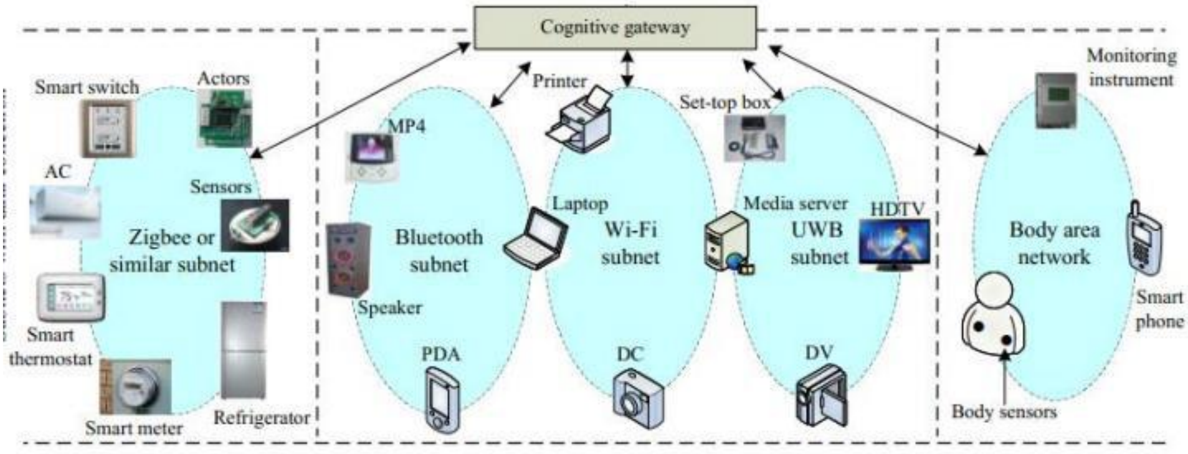

Figure 4.2 (Various networks in smart home)

A cloud solution provides benefits in the form of increased computer processing power and data storage capacity. In addition, it releases the user from the task of installing, updating and backing up software on the centralized automated home server. In the near future it is also likely that device information can be retrieved online for easy device setup of similar devices.

4.1. Use of Sensors and actuators

In smart homes sensors are the primary source for information of user activity. This information is used by the artificial system to get a fragmented picture of the user current activity. Sensor technology has evolved through the last decades and till date small integrated low-power sensors exist. So, the challenges to find which sensors are the most suitable for smart homes, how will the measured data be used, and where should they be installed. Location sensors are normally used to detect a change in context state caused by the user. For example, if the user takes a cup from the cupboard a sensor registers this. In general, location sensors are members of the groups: Simple switches, pressure mats, passive infrared detectors, radar, sound, light, and camera based sensors. Camera based sensors are not used much in smart homes, because users consider them to be too invasive. In addition they produce a huge amount of data that needs to be processed and transferred to the artificial system. Sound (including ultrasound) and light sensors are used too, but they suffer from considerable costs, high current consumption, using comprehensive processing resources, and detection uncertainty compared to simple switches. However, they are able to provide high resolution contextual measurements.

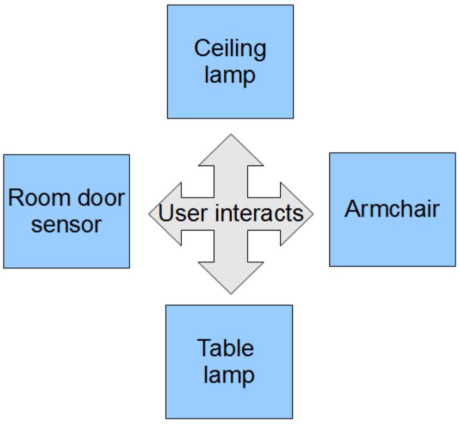

Figure 4.3 (A simple Smart home (Living Room))

5. Proposed methodology and framework

The methodology initially thought of is based on intensive imagination as well as theory of induction and deduction, combined with an iterative process model to support the research process. It may also be planned to use technical and mathematical analysis based on library and online searches, code implementation and testing by using empiric dataset.

The features of the framework may be with simplified implementation, high flexibility, learning and prediction on the fly, advanced temporal prediction, standalone capability, limited processing resources, and easy integration with the smart objects. The smart objects and sensors contained in a smart home must be able to communicate with each other and the outside world. At the high OSI-layer level smart objects need to exchange information such as setup information and predicted actions. This is supported by the middleware layer. The lower layers, which are needed to support the higher layer information exchange, take care of the actual information transport through the physical media.

5.1. Problem motivation

Building automation has been a research field for the last two decades and has contributed with many standards, theories and technologies. Throughout the years building automation has developed from performing simple controlled functions such as regulating the heating, ventilation, and air conditioning to handling the changing needs throughout its lifecycle.

Now a day, building automation covers an umbrella of network and computerized technologies that are integrated into commonly available building management systems.

From this technological era, the concept of application of artificial intelligence and Internet of Things in home automation may be visualized. The purpose is to ease life for its residents by controlling mundane functions such as light, ventilation, heat and appliances to improve comfort, convenience, and energy efficiency in the automated homes. It can be performed in a non-autonomous way by adding simple remote controlled, timer based and pre programmable functions.

(i) The principles of intensive imagination generally may use the external changing conditions as an empowerment which may support the understanding of an experimenting approach. It means that the process of exploring, researching and experimenting should adapt to the changing external conditions in the form of adjusting processes and methods used, planning, and decisions. In this case, based on the present knowledge level, as the research progresses more knowledge may be provided, the new knowledge may then guide the adjustments for the future processes and methods.

(ii)The principles of induction and deduction help to generalize a theory by removing the special attributes, i.e., transforming a subjective theory into a more objective one. Using the principle of induction may directly aim to draw conclusions based on specific examples and hypotheses. Sometimes induction may lead to a wrong conclusion. So to find the correct way to deal with this risk is to combine it with common sense. Common sense helps to choose and find the right path in the possible choices. The induction principle may be used in the methodology of this work where it may provide a theory based on data from simulated smart home components mathematical derivations, library researches and internet explorations.

5.2. Problem definition

While representing smart home, four main challenges may be occurred which are high cost of ownership, inflexibility, poor manageability, and difficulty in achieving security. The main objective in this work is to design the mechanism for smart home using Internet of Things capable of controlling and automating most of the house appliances through an easy manageable web interface. It should have a great flexibility by using high bandwidth internet as well as Wi-Fi technology to interconnect its distributed sensors to the primary server.

5.3. Simulation Model with basic design principle

Cloud computing is the practice of using remote servers on the internet to manage, store and process data instead of using a personal computer. Cloud computing is a general term that is better divided into three categories: Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service. IaaS (or utility computing) follows a traditional utilities model, providing servers and storage on demand with the consumer paying accordingly. PaaS allows for the construction of applications within a provider’s framework, like Google’s App Engine. SaaS enables customers to use an application on demand via a browser. A common example of cloud computing is Gmail, where the stored data can be accessed from any computer with internet access. Generally Gmail is used for the storage of the data.

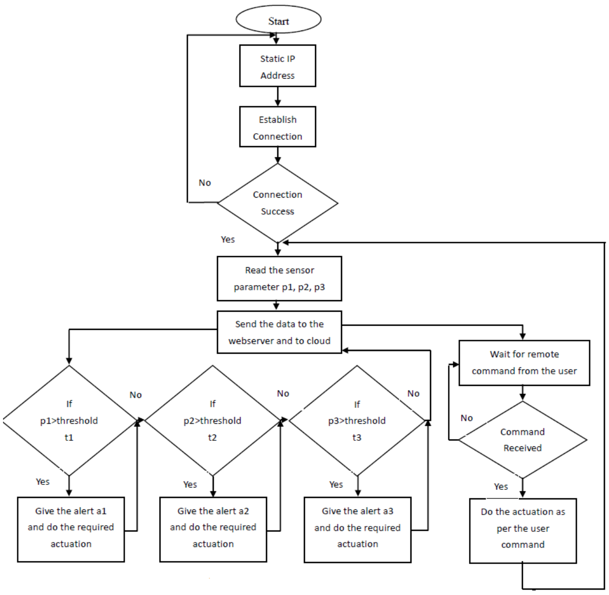
Start
Static IP Address
Establish Connection
No
Connection Success
Yes
Read the sensor parameter p1, p2, p3
Send the data to the webserver and to cloud
Wait for remote command from the user
No
Command Received
Yes
Do the actuation as per the user command
If p1>threshold t1
No
Yes
Give the alert a1 and do the required actuation
If p2>threshold t2
No
Yes
Give the alert a2 and do the required actuation
If p3>threshold t3
No
Yes
Give the alert a3 and do the required actuation

Figure 5.1 (Activities related to Smart home)

ISSN: 2321-8363
Impact Factor: 5.515

The flow chart shown in figure 5.1 represents the activities in the system. The sensor parameters may start reading the parameters as soon as the connection may be established. The sensor data are sent to the web server and stored in the cloud. The data can be analyzed anywhere any time. If the sensor parameters are greater than the threshold level then the respective alarm may be raised and the required actuation may be done for the controlling of the parameters.

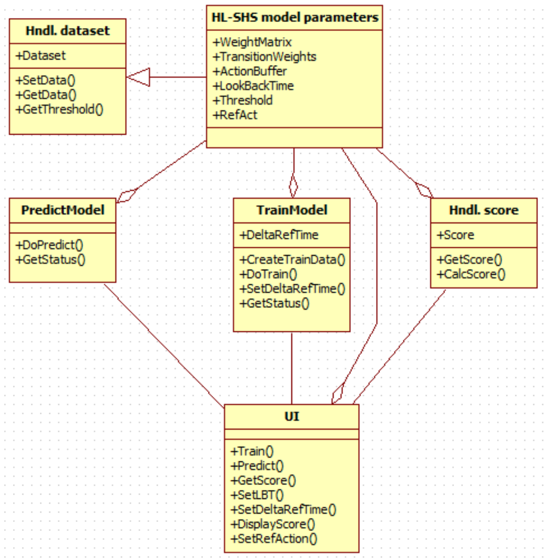

Figure 5.2 (Smart home Model (Class diagram))

A Unified Modeling Language (UML) based class diagram for the smart home simulator model is shown in the figure 5.2. The principles of the Object Orientated Method are used in the design of this model. This enables the possibility to encapsulate common functionality, which reduces coupling between objects and uses OMT principles, such as generalization and
polymorphism. The central attributes are allocated in the model class. Using this principle ensures that the model context is decoupled from the model itself, but that the dataset is still available for the model classes. These classes are tightly coupled to the model parameters by the used aggregation. This tight coupling is necessary because it combines the data and the method.

HTML is a format that tells a computer how to display a web page. The documents themselves are plain text files with special "tags" or codes that a web browser uses to interpret and display information on your computer screen. HTML stands for Hyper Text Markup Language; an HTML file is a text file containing small markup tags. The markup tags tell the Web browser how to display the page. An HTML files must have an htm or html file extension. The proposed smart home may be modelled using a model developed using ASP .NET and java script library which may run on a personal computer. Datasets to feed this model may be derived from a real-world setting. This is important for reflecting the real-world uncertainties and sensor noise in the datasets. These elements are vital in testing algorithms to ensure that they are able to filter out the correlated information and are able to converge in the learning process.

jQuery is the JavaScript library for building Ajax based web applications. The problem with jQuery is written primarily for desktop applications and doesn't have many of the features desired for mobile applications, that is where jQuery Mobile comes into play. jQuery Mobile is a framework built on top of jQuery and it address the mobile gaps of jQuery.

ASP.NET is a framework for building scalable, standards-based web applications using well-established design patterns. The required framework is also great for building mobile web applications with jQuery Mobile. Similarly the search engine in particular is useful to mark duplicate entries.

All jQuery Mobile sites require references to the jQuery JavaScript file and the jQuery mobile JavaScript file. In HTML5, the <meta> tag may be used to define metadata for the HTML document. The <meta name="viewport"/> meta tag is used to control how HTML content will appear in mobile browsers so that the content is sized correctly for the device.

The jQuery Mobile framework uses HTML5 "data-" attributes to allow for markup-based initialization and configuration. The data attributes allow to add simple metadata to individual elements that are interpreted by the jQuery Mobile JavaScript functions.

With the jQuery Mobile app, most of the code may be running locally on the device. A controller method may be cited in this case that will run on the server to talk to the Net.

The jQuery Mobile app runs on multiple devices with different mobile operating systems.

6. Steps while designing storage engine

Step 1 : MySQL provides support for many storage engines which manage storage and retrieval.
MyISAM and InnoDB are common. On table creation engine can be specified. A basic storage engine allows read only tables. Most engines read data from files and feed to MYSQL. On the other hand, our idea is to retrieve data from API’s and feed it to MYSQL. This will allow us to conduct complex analysis using sql on data retrieved from API’s. The idea is to write an engine for each set of related API’s.

Step 2 : The mysql storage engine retrieves data from Gmail and feeds to mysql.

Step 3: When user enters a select query on Email table, the control passes to EmailSearchEngine in rnd_init method.

This method checks that table name is really “Email”. Then it checks that where clause parse tree is present or not. If yes, then where clause parse tree is traversed to be converted to IMAP search commands. Otherwise all emails in the inbox are fed to MySQL. To retrieve emails specific software only being used for C++ and .NET Windows programmers get a very versatile library to send and download emails via SMTP, POP3 and IMAP with TLS and SSL support.

Step 4 : Dynamically add access database columns at runtime using vb.net

Step 5 : Storing complex properties as text in database

Step 6 : Database Setup

First, look at the table schema of Blogs table: For example, create table Blogs (BlogId int Primary Key identity,

Url nvarchar(4000)not null,

Tags navchar(4000),

Owner navchar(4000));

Insert into Blogs(Url, Tags, Owner) values

('http:blogs.msdn.com/dotnet','[".net", "core", "c#"]','{"Name": "Asit", "Surname": "Dash", "email ": dashasit@mail.com});

Step 7 : Mapping columns to properties

In order to map Tags and Owner columns, it may be needed separate properties for them. It may be also be required to add two internal _Tags and _Owner properties to map the columns. These two fields may contain text taken from database. It may be an utility class that is used to define properties in Owner property, it is not mapped to database table.

6.1. Components

The minimum components may be required in the smart home Simulation are:

(i) Two RaspberryPi 2 model B: The main processing and controlling unit of the system. One was used for the room model and the other for the surveillance car.
(ii) Servo Motor: It acts as the door lock.
(iii) Infrared (IR) sensor: Shows the current state of the front door, either opened or closed.
(iv)Web Camera: Acts as a surveillance camera for the room streaming images of that room that are processed by the RaspberryPi. It utilizes OpenCV's image processing to be able to detect objects in the room.
(v) Smoke Detector: It detects _re, ensuring the safety of the home.
(vi)Two H-Bridges: Each H-Bridge controls two motors, two are used to control the four DC motors of the device.
(vii)Wi-Fi Dongle: Attached to the Raspberry Pi through USB port to allow its connection to wireless internet instead of using Ethernet cable.

7. Performance evaluation

The existence of the heterogeneous wireless network sometimes may highly affect the performance of the smart home entities. The interference mainly may affect the communication between sensors and sensor and coordinator. To evaluate the interference avoidance as well as the smart energy management system under the interference of a WIFI AP, two WIFI APs and several ZigBee sensors may be considered. Each household appliance should be connected with a sensor, which is further connected with a ZigBee coordinator. The ZigBee coordinator may be responsible for aggregating data from the sensors attached to each appliance and send it to the management station. Each home user may be continuously generating unicast data packets to the WIFI AP. Similarly, the same environment may be tested with a relay and pure WSN based networking.

8. Discussion and future direction

There are so many ways to determine the architectural structure of the IoT. The network architecture as well as visualization associated with IoT applications may provide significant value to the whole system which will help to escalate more efficiently. Each one of the IoT components of the different layers may be associated with separate technologies and, therefore, distinct weaknesses are found based on functionality and application. In the present scenario, IoT needs a clear analysis and vision to strengthen its foundations towards a secure environment. Further analysis towards confidentiality, integrity and availability regarding the same may be more essential.

9. Conclusion

In the present scenario, the Internet of Things state can make previously unknown but significant work in secured embedded computer devices. But sometimes, publicly-known security may breach initiation vectors point to vulnerable or neglected IoT devices. As a result the number of records stolen may be continued to grow. The amount of data handled by IoT devices may soar at exponential rates, which means higher exposure of sensitive data and brings up the need to foster discussions among security researchers. Recent efforts have not been able to cover the entire security spectrum, which reveals research opportunities in different areas including smart object hardening and detection capabilities. Current issues and challenges should be taken as improvement opportunities that need to be achieved under a rigorous process that incorporates security objectives at early design stages and efficient and effective application of security standardized solutions at production stages.

References

[1] Normann, A. & Jamison, A., 2011. Knowledge Making in Transition. On the Changing Contexts of Science and Technology. University of Pittsburgh Press.

[2] Wang, S., 2010. Intelligent Buildings and Building Automation. 2nd ed. New York: Spon press.

[3] Xiaojuan, Z., 2010. he Strategy of Smart Home Control System Design based on Wireless Network. International Conference onComputer Engineering and Technology (ICCET), pp.4-37 to 4-40.

[4] Mingyi, M., Qian, M.Q., Jianjun, L. & Zhicheng, C., 2010. Solution to Intelligent Management and Control of Digital Home. In International Conference on Biomedical Engineering and Informatics (BMEI)., 2010. IEEE Conference Publications.

[5] Basil Hamed, "Design & Implementation of Smart House Control Using LabVIEW" at International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, January 2012

[6] Basma M. Mohammad El-Basioni1, Sherine M. Abd El-kader2 and Mahmoud Abdelmonim Fakhreldin3, "Smart Home Design using Wireless Sensor Network and Biometric Technologies" at Volume 2, Issue 3, March 2013

[7] C. Dixon, R. Mahajan, S. Agarwal, A. Brush, B. Lee, S. Saroiu, and P. Bahl, An Operating System for the Home, *NSDI*, 2012.

[8] J. Deng, R. Han, and S. Mishra, Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks, *Proc. of ACM/IEEE IPSN*, 2006. pp. 292-300.

[9] S. Ravi, A. Raghunathan, S. Chakradhar. Tamper Resistance Mechanisms for Secure, Embedded Systems, Proc. of 17th International Conference on VLSI Design, 2004. p. 605.

[10] S. Munir, J. Stankovic, C. Liang, and S. Lin, New Cyber Physical System Challenges for Human-in-the-Loop Control, *8th International Workshop on Feedback Computing*, June 2013.

[11] TRUSTe, "Internet of Things Industry Brings Data Explosion, but Growth Could be Impacted by Consumer Privacy Concerns," TRUSTe Research, 29 05 2014. [Online]. Available: http://www.truste.com/blog/2014/05/29/internet-of-things-industry-brings-data-explosion-but-growth-could-be-impacted-by-consumer-privacy-concerns/. [Accessed 16 20 2014].

[12]"Fortinet Reveals "Internet of Things: Connected Home" Survey Results," Fortinet , 23 June 2014. [Online]. Available: http://www.fortinet.com/press_releases/2014/internet-of-things.html. [Accessed 15 10 2014].

[13] H. Gross; M. Holbl, D. Slamanig, and R. Spreitzer, "Privacy-Aware Authentication in the Internet of Things," *Cryptology and Network Security. Springer International Publishing*, pp. 32-39, 2015.

[14] M. Maroti, B. Kusy, G. Simon, and A. Ledeczi, The Flooding Time Synchronization Protocol, *ACM SenSys*, November 2004

[15] K. Tsui, D. Kim, A. Behal, D. Kontak, and H. Yanco, I Want That : Human-in-the-Loop Control of a Wheelchair-Mounted Robotic Arm. *Journal of Applied Bionics and Biomechanics 8,* 2011.

[16] R. Acharya and K. Asha, "Data integrity and intrusion detection in wireless sensor networks," in Networks, 2008. ICON 2008. 16th IEEE International Conference on, pp. 1–5, IEEE, 2008.

[17] D. Uckelmann, M. Harrison, and F. Michahelles, An architectural approach towards the future internet of things. Springer, 2011.

[18] K. on Security, "Ddos on dyn impacts twitter, spotify, reddit," 2016.

[19] O. Vermesan and P. Friess, Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers, 2013.

[20] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, no. 9, pp. 51–58, 2011.

[21] L. Tan and N. Wang, "Future internet: The internet of things," in 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 5, pp. V5–376, IEEE, 2010.

[22] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for internet of things (iot)," in Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on, pp. 1–5, IEEE, 2011.

[23] S. H. Hong, M. Yu and X. Huang, "A real-time demand response algorithm for heterogeneous devices in buildings and homes," *Energy*, vol. 80, pp. 123-132, 2015.

[24] S. Rani and S. Ahmed, "Multi-hop Routing in Wireless Sensor Networks: An Overview, Taxonomy, and Research Challenges," Springer, 2016.

ISSN: 2321-8363
Impact Factor: 5.515

A Brief Author Biography

Prof. Jyoti Prakash Mishra– Prof. Jyoti Prakash Mishra is having more than 20 Years of experience in the field of Engineering as well as in Industries in India and abroad.

Dr. Sambit Kumar Mishra – Dr. Sambit Kumar Mishra is having 20 Years of experience in teaching in different Engineering Institutions in India. He is member of different professional bodies, i.e. ISTE, IAE, CSTA, IACSIT. He is also member of editorial board of some peer reviewed and indexed Journals.