IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Special Issue-3, May 2016 E-ISSN: 2347-2693

Internet of Things: Smart College

Swaroopa P T[1], Mrs. Chaitra H K [2]

[1]Department of computer Science & Engineering
[2]Department of Computer Science & Engineering, SJBIT Bengalure, India

Available online at: www.ijcseonline.org

***Abstract*—**The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Concept of smart college can one be of the emerging trend in IoT in coming up years where the thought of 'Smart Campus, Secure Campus' may become the new mantra. The vision of such an Internet Of Things (IoT) system, supported by private industries and governments globally will have the potential to mark an evolution in the way concept of education is viewed currently and will surely have a great impact on our environment and our lives. This paper hence provides an comprehensive thought and survey on enabling and using of IoT technologies in the educational institutions, Furthermore, the paper will present and discuss an idea about smart college using the concepts of IoT.

***Keywords*—** Internet of Things (IoT), device-to-device (D2D), Machine-to-Machine (M2M), Radio frequency identification (RFID), IoT standardization.

I. INTRODUCTION

Internet of Things (IoT) is a recent communication paradigm that envisions a near future, in which the objects of everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, forming a digital skin [1]. The IoT concept, hence, aims at making the Internet even more immersive and pervasive. Various applications of IoT such as smart switches home automation, a smart irrigation in agriculture etc. have already made it into the market and are building basic foundation to the concept of smart planet which might be the future of earth in upcoming days. These thoughts will aid the development of a number of applications that make use of the enormous amount and variety of high resolution data generated by the day to day objects around us, helping in decision making process at many levels.

The IoT finds application in many different domains, such as home automation, industrial automation, medical aids, mobile healthcare, intelligent energy management and smart grids, traffic management and many others. Such a heterogeneous field of application makes the identification of solutions capable of satisfying the requirements of all possible application scenarios a formidable challenge. Therefore, from a system perspective, the realization of an IoT network, together with the required backend network services and devices, still lacks an established best practice because of its novelty and complexity. In addition to the technical difficulties, the adoption of the IoT paradigm is also hindered by the lack of a clear and widely accepted business model that can attract investments to promote the deployment of these technologies. This idea of smart college will clearly affect the thoughts of millions regarding the IoT technologies. By making the young generation familiar with the application of IoT it becomes easy to adopt the concept in a larger scale.

II. ELEMENTS OF IoT

By taking reference of the emerging technology of Smart City services which are based on a centralized architecture [6]. It will be easy to view the idea of smart college at application level. Here we use a dense and heterogeneous set of peripheral devices deployed over the campus area to generate different types of data based upon the type of application .These data are then delivered through suitable communication technologies to a centralized facility, where data storage and processing are performed. The different component of a college IoT will require the deployment of suitable protocol layers in the different elements of the network. The key element of the architecture, the link layer technologies that can be used to interconnect the different parts of the IoT will also be discussed.

A. *Web Technology for IoT Architecture:*

In the IoT domain many different web standards are still struggling to be the final reference one in the smart college application we focus specifically on IETF standards because they are open and royalty-free, are based on Internet best practices, and can count on a wide community of network designers, operators, researchers and vendors.

The urban IoT system, provided that they are capable of interfacing with all the layers we can distinguish three distinct functional layers:

1) *Data Format:* As mentioned, the smart college IoT paradigm sets specific requirements in terms of data accessibility. If the architecture chosen is based on web services, data exchange is typically accompanied by a description of the transferred content by means of semantic representation languages, of which the eXtensible Markup Language (XML) is probably the most common. But because of the size of XML messages is often too large for the limited capacity of typical devices for the IoT.

2) *Application and Transport Layers:* Most of the traffic that crosses the Internet nowadays is carried at the application layer by HTTP over TCP. However, the complexity of native HTTP makes it unsuitable for a straight deployment on constrained IoT devices. For such an environment, in fact, the human-readable format of HTTP, which has been one of the reasons of its success in traditional networks, turns out to be a limiting factor due to the large.

3) *Network Layer:* IPv4 is the leading addressing technology supported by Internet hosts. However, IANA, the international Protocol stacks for unconstrained and constrained IoT nodes can also be used.

B. *Link Layer Technologies*

A system for smart college IoT if established at a university level then because of its deployment area size, requires a set of link layer technologies that can easily cover a wide geographical area and, at the same time, support a possibly large amount of traffic resulting from the aggregation of an extremely high number of smaller data flows.

C. *Devices:*

The devices that are essential to realize an urban IoT, classified based on the position they occupy in the communication flow. Bluetooth SIG, adopted bluetooth Core Specifications Available:

1) *Backend Servers:* At the root of the system, we find the backend servers, located in the control center, where data are collected, stored, and processed to produce added- value services. In principle, backend servers are not mandatory for an IoT system to properly operate, though they become a fundamental component of an urban IoT where they can facilitate the access to the smart city services and open data through the legacy network infrastructure. Backend systems commonly considered for interfacing with the IoT data feeders include the following.

2) *Database management systems*: These systems are in charge of storing the large amount of information produced by IoT peripheral nodes, such as sensors. Depending on the particular usage scenario, the load on these systems can be quite large, so that proper dimensioning of the backend system is required.

3) *Web sites*: The widespread acquaintance of people with we interfaces makes them the first option to enable interoperation between the IoT system and the "data consumers," e.g., public authorities, service operators, utility providers, and common citizens.

4) *Resource planning systems (RPS):* RPS components support a variety of business functions and are precious. Tools that are used to manage the flow of information across a complex organization such as college administration are few of resource planning systems. Interfacing RPS components with database management systems that collect the data generated by the IoT allows for a simpler management of the potentially massive amount of data gathered by the IoT, making it possible to separate the information flows based on their nature and relevance and easing the creation of new services.

5) *Gateways:* Moving toward the "edge" of the IoT, we find the gateways, whose role is to interconnect the end devices to the main communication infrastructure of the system. With reference to the conceptual protocol architecture depicted the gateway is hence required to provide protocol translation and functional mapping between the unconstrained protocols and their constrained counterparts, that is to say XMLEXI, HTTP-CoAP, IPv4/v6-6LoWPAN.

III. SMART COLLEGE

The Internet of Things describes a world in which everyday objects are connected to a network so that data can be shared. Many of us already carry 'smart' phones with us to college, but a phone is not smart. It helps its user to make smarter decisions. Smartphones are only the beginning. In the future of IoT we will carry sensors that will automatically enter our attendance, automated library system and also help in how we move around in the college environment.

For the Internet of Things to flourish, interoperability must apply across all parts of the system, including the transmission networks and the data being transmitted. Data and devices must have proportionate "security by default". Standards must protect against cybercrime and security threats, in our case attendance forgers and help to ensure that the system is trustworthy and trusted by those who make the system. They should also support energy efficiency, as this will help increase the range of potential applications and manage the burden on energy supply. In today's college system much of the data released to date is enabled to be human-readable, and not machine-readable. This needs to be changed step by step to establish a digital skin over the college campus.

- *Smart Library System:* In order to properly regulate the library system each book is embedded with sensors which will make the library system more convenient for use·
- *Smart Attendance:* using technologies like face recognition system, the attendance of each ward can be precisely regulated.
- *Smart administration:* With the precise data available on each student it will be easy for the administration to plan and meet various industry standards.
- *Smart Monitoring:* Monitoring of the elements in the system is very much necessary in order to accomplish certain goals in an organization. Hence with sensors collecting real time data and making real time decision easy, it will be easy to achieve those goals.
- *Smart Tracking:* Students who use various forms transport facility including the school bus tracked until he/she reaches home safely. Time of departure, arrival and journey.
- *Smart Security*: An smart card with sensors and technologies that can be used to alert the school authorities in case of any emergency will add great value for students who commute.

The Internet of Things already poses challenges in the sensitive area of personal identity and privacy. The scale of personal information, particularly location and financial information, which is collected by existing technology, is huge. This data collected will only increase as we use more and more Internet of Things technologies. Hence proper handling of these data is very much necessary.

In order to establish the smart college system we will need various kinds of communications of types such as:

- Wi-Fi: The IoT will require primarily wireless communications. As a result, we expect Wi-Fi to be the key communications standard for IoT, much like DSL/Ethernet was for the fixed Internet and 3G/4G for the mobile internet·
- Cellular: In an IoT world, no device will be left off the network. Cellular connections will be needed for hard to reach or mobile objects (e.g., cars or identity wristbands). Computing where data is stored outside of your local device, often on servers in large data centers sometimes thousands of miles from where the data was generated. But in the age of the IoT, we expect more of the network intelligence to reside closer to the source: what technologists call the network edge or the "fog". Look for the rise of fog computing architectures, as most data will be too noisy or latency-sensitive (think: it needs to get there and back super-fast) or expensive to be carried all the way back to the cloud. In the age of the IoT, in order to sense the surrounding we shall need various sensors and low-cost microcontrollers points and power requirements relative to traditional semiconductor architecture.

IV. ARCHITECTURE OF IoT

The IoT system will be an example of event driven architecture, bottom-up made (based on the context of processes and operations, in real-time) and will consider any subsidiary level. Therefore, model driven and functional approaches will coexist with new ones able to treat exceptions and unusual evolution of processes (Multi-agent systems, B- ADSc, etc.). In an Internet of Things, the architecture of IoT consists of four main layers:

1) Application.
2) Management service layer.
3) Gateway and network layer.
4) Sensor layer.

A. Application Layer :

Application layer provides user interface for using IoT; it can be in form of mobile application or any type of graphical interface. Different applications for various sectors like Transportation, Healthcare, Agriculture, Supply chains, Government, Retail etc. are available and proper GUI for accessing these applications is available.

B. Management Service Layer:

This layer is responsible for capturing the capturing of periodic sensory data. That is got from various different resources. From the raw data obtained relevant information is extracted using certain data analytics. Along with the Streaming Analytics is for processing real time data got from the sensors and satellites etc. this layer also ensures security and privacy of data.

C. Gateway and Network Layer:

Gateway and network layer provides robust and high performance network Infrastructure which supports the communication requirements for latency, bandwidth or security. It also allows multiple organizations to share and use the same network independently.

D. Sensor layer:

This is the lowest Abstraction Layer in the architecture of IoT, which is incorporated to measure physical quantities, interconnects the physical and digital world.it also collects and process the real time information.

Communication within the IoT:

Various types of communication may exist within the IoT, and these include D2D, device to human and vice versa, and device to distributed storage. Communication could be within the same network (intra-domain) or across heterogeneous networks (inter-domain) [8].A constrained network may be one of the following:

1) Short-range wireless network: This includes the IEEE 802.15 standards for wireless personal area networks (WPANs) and the IEEE 802.11 standards for wireless local area networks (WLANs).
2) Low-power loss network (LLN): This is a low-bit-rate WPAN under the IEEE 802.15.4 standards.
3) Delay-tolerant network: This is deployed in performance challenged environments where continuous end-to-end connectivity cannot be assured. Such environments are spacecraft, natural disaster situation, or underwater.
4) WSNs: These are made up of sensors that have been densely and randomly deployed to capture information, e.g., humidity or motion. The sensors have low power and self- organizing and collaborative capabilities.

5) Cellular Networks: wireless wide area networks such as third-generation, fourth-generation, and long-term evolution networks.
6) WiMAX: IEEE 802.16 standards for wireless metropolitan area networks (WMANs).

V. BENEFITS OF SMART COLLEGE

The benefits of using IoT within campus come with its own sets of advantages and disadvantages. With the introduction of IoT the college campus know to the students before this will be completely different because of the technology that will be used.one will be monitored and can monitor each and every act of other. Advantages of Smart campus:

1) Help utilize energy efficiently:

Internet of things can help in reducing the consumption of various resources used within the college in efficient manner helping to save the energy. With various devises such as automated lightning and air conditioning large amount of energy can be saved from wasting.
Also by using accurate sensors and automated systems the college has to only pay for resources that are actually being used.
Eg: like switching on the lights of classes in sessions are going on.

2) Improve the Quality of Education:

The Internet of things if used in the field of education will not only have a major impact on the system but will also affect the quality of the education being received by the thousands of the students.
The new trend of online education can be launched in full magnitude with the support of IoT, where students from any rural place can listen to one live lecture by sitting at their own place. This will promote the scope of opportunity for rural area students in a very good manner.

3) ImproveSecurity:

Living within IoT exposes the system into a large range of attacks. Hence the systems should be properly de-perimeter in order to teach the system on who to trust and not. This becomes one of the main considerations with security of data issue.

IoT currently is being used in various fields. Few of them are:

1) *IoT Infrastructure for Smart City*
As the key technological enabler, IoT is introduced from three different domains: network-centric IoT, Cloud-centric IoT, data-centric IoT, corresponding to communications, management, and computation requirements of smart city development and deployment.

2) *Using IoT in the healthcare service industry:*
IoT provides new opportunities to improve healthcare. Powered by IoT's ubiquitous identification, sensing, and communication capacities, all objects in the healthcare systems (people, equipment, medicine, etc.) can be tracked and monitored constantly. Enabled by its global connectivity, all the healthcare-related information (logistics, diagnosis, therapy, recovery, medication, management, finance, and even daily activity) can be collected, managed, and shared efficiently. For example, a patient's heart rate can be collected by sensors from time to time and then sent to the doctor's office.

3) *Using IoT in FSC:*

A typical IoT solution for FSC (the so-called Food- IoT) comprises three parts:

a) The field devices such as WSN nodes, RFID Readers/tags and user interface terminals, etc.

b) The backbone system such as databases, servers, and many kinds of terminals connected by distributed computer networks, etc.

c) The communication infrastructures such as WLAN, cellular, satellite, power line, Ethernet, etc. As the IoT system offers ubiquitous networking capacity, all of these elements can be distributed throughout the entire FSC. Furthermore, it also offers effective sensing functionalities to track and monitor the process of food production.

4) *Using IoT for safer mining production:*

Mine safety is a big concern for many countries due to the working condition in the underground mines. To prevent and reduce accidents in the mining, there is a need to use IoT technologies to sense mine disaster signals in order to make early warning, disaster forecasting, and safety improvement of underground production possible. By using RFID, Wi-Fi, and other wireless communications technology and devices to enable effective communication between surface and underground, mining companies can track the location of underground miners and analyze critical safety data collected from sensors to enhance safety measures. Another useful application is to use chemical and biological sensors for the early disease detection and diagnosis of underground miners, as they work in a hazardous environment. More research is needed regarding safety characteristics of IoT devices used in the mining production.

5) *Using IoT in transportation and logistics:*

IoT will play an increasingly important role in transportation and logistics industries. As more and more physical objects are equipped with bar codes, RFID tags or sensors, transportation and logistics companies can conduct real-time monitoring of the move of physical objects from an origin to a destination across the entire supply chain including manufacturing, shipping, distribution, and so on . Furthermore, IoT is expected to offer promising solutions to transform transportation systems and automobile services In the near future, we will see the development of an automotive autopilot that can automatically detect pedestrians or other vehicles and take evasive steering to avoid collisions .

6) Using IoT in firefighting:

IoT has been used in the firefighting safety field to detect potential fire and provide early warning for possible fire disasters. In China, RFID tags and/or bar codes are being attached to firefighting products to develop nationwide firefighting product information databases and management systems. By leveraging RFID tags, mobile RFID readers, intelligent video cameras, sensor networks, and wireless communication networks, the firefighting authority or related organizations could perform automatic diagnosis to realize real-time environmental monitoring, early fire warning and emergency rescue as needed.

VI. CONCLUSION

In this paper, the various currently available trends for the implementation of IoT and its applications were addressed. The discussed technologies are close to being standardized, and industry players are already active in the production of devices that take advantage of these technologies to enable the applications of interest, such as those described in Smart College.

In fact, while the range of design options for IoT systems is rather wide, the set of open and standardized protocols is significantly smaller. The enabling technologies, furthermore, have reached a level of maturity that allows for the practical realization of IoT solutions and services, starting from field trials that will hopefully help clear the uncertainty that still prevents a massive adoption of the IoT paradigm. An idea regarding the smart college will in near future realize to be true in Indian colleges which will in turn result in an smarter education system, but an active participation of government is very much necessary to promote such ideas.

VII. REFERENCE

[1] Intelligent Device-to-Device Communication in the Internet of ThingsOladayo Bello, Member, IEEE, and Sherali Zeadally, Senior Member, IEEE.december **2013**

[2] Pranay Kujur and Kiran Gautam, "Smart Interaction of Object on Internet of Things", International Journal of Computer Sciences and Engineering, Volume-03, Issue-02, Page No (15-19), Feb -2015,

[3] Internet of Things in Industries: A Survey Li Da Xu, Senior Member, IEEE, Wu He, and Shancang Li.november **2014**

[4] Securing the Internet of Things:A Standardization Perspective Sye Loong Keoh, Sandeep S. Kumar, and Hannes Tschofenig.June **2014**

[5] An Information Framework for Creating a Smart City through Internet of Things Jiong Jin, Member, IEEE, Jayavardhana Gubbi, Member, IEEE, Slaven Marusic, and Marimuthu Palaniswami, Fellow, IEEE.April **2014**

[6] Andrea Zanella, Senior Member, IEEE, Nicola Bui, Angelo Castellani,Lorenzo Vangelista, Senior Member, IEEE, and Michele Zorzi, Fellow, IEEE" Internet of Things for Smart Cities" IEEE internet of things journal, vol. 1, no. 1, february **2014**

[7] Internet of Things for Remote Healthcare , "P K Mishra, M. R Pradhan and M.Panda", International Journal of Computer Sciences and Engineering, Volume-04, Issue-04, Page No (106-111), Apr -2016,

[8] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey,"Comput. Netw., vol. 54, no. 15, pp. 2787–2805, **2010.**