SMART INSTITUTIONS

Digital Future with IoT

Dr. Shalini Vermani

Associate Professor, Apeejay School of Management

Abstract: Internet of Things (IoT) is a futuristic vision of the world where everything is linked by means of appropriate information and communication technology, to enable a new set of applications and services. IoT has changed the way we think and implement things in our life. For the learners of the 21st century, conventional institutions and classical teaching methods in classroom are no more attractive. With IoT, future institutes will become smart institutes. It will provide a new platform of teaching and learning to the educators and learners of modern era.

Keywords: IoT, Fog Computing, Smart Devices.

1. Introduction

IoT is an emerging technology. In this, sensors are embodied in a wide range of networking products which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities to existing technologies such as making vehicles smart to monitor the heartbeat of the driver, advance navigation system, self-driven vehicles etc. The large-scale implementation of IoT devices promises to transform multiple aspects of life. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management components transform the traditional house into a 'smart home', offering more security and energy efficiency. Personal IoT devices like wearable fitness and health monitoring devices and network enabled medical devices are transforming the way healthcare services are delivered. IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges helps in transforming the cities into 'smart cities', which help minimize congestion and energy consumption. IoT technology helps in transforming agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors.

With the change in the time, humans evolved its way to live, with enhanced communication methods to high tech super intelligent machines, which not only changed the way of living but also opened doors for transforming the existing methods to adapt the new changes.

IoT helps us to introduce another level of that vision which is seen by many tech giants such as Google and Microsoft to motivate the world and transform it into the technical utopia for human beings. This technology not only brings solutions to our complex lives but also opened doors for many new unexplored opportunities. With IoT, traditional devices are modified and connected to the internet granting them the ability to communicate with each other, sharing information and handling the daily problems on their own without any human intervention. This technology has the most prominent examples such as smart homes, smart grids, connected cars and this list goes on.

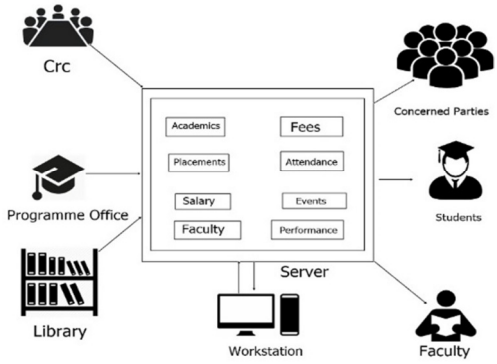
Knowledge distribution has changed from the traditional gurukuls to the modern-day schools and institutes, now it is time to upgrade the knowledge systems and to transform the present-day institutions into **'Smart Institutions'.**

In Smart Institutions, physical devices will communicate with each other without any human intervention which will result in faster and timely output. Smart Institutions will increase comfort, convenience and better management which is a step toward the improvement of quality of education and campus life. This paper tries to find out more possibilities of Smart Institutions under IoT umbrella.

The paper discusses the concept of Smart Institution with the incorporation of IoT devices having intelligence embedded sensors. These Smart Institutions will improve the speed and efficiency of data exchange. IoT encourages the communication of connected devices, because of this the physical devices will be continuously connected to each other and total transparency can be achieved with prominent efficiencies and greater quality. However, IoT also face some issues and challenges that need to be considered and properly addressed.

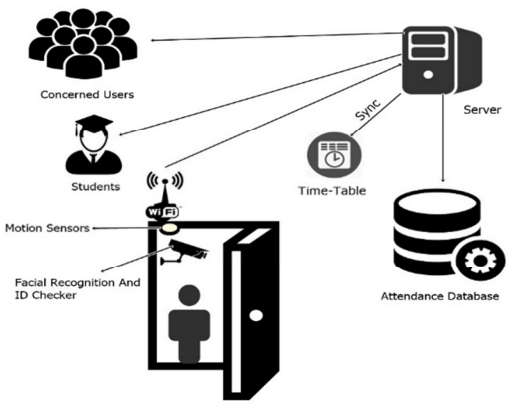
II. Application of IoT in Smart Institution

(i) Smart Office



IoT powered administrative offices will enhance the quality of work of the institutes, these offices will be equipped with smart screens and data managing servers, which will provide live streaming and on demand access to any office related information such as academic, fee, placement, attendance and performance etc. Similarly. Faculty and staff can access the relevant information.

(ii) Automatic Attendance System

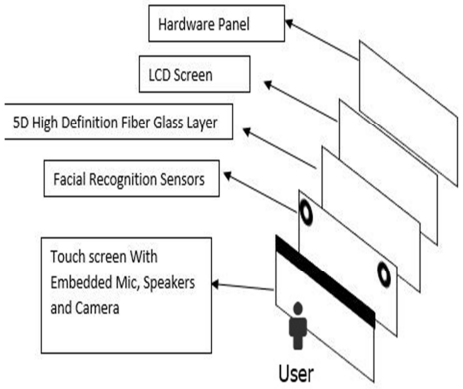


With IoT, there will be automatic attendance system. Attendance of faculty and staff will be captured by the facial scanners on the entry gate and attendance of students will be captured for each class.

For faculty and staff, sensors embedded on the gate identifies the person through facial recognition, the system then look up for the records into the server and on finding an appropriate match, the attendance will be automatically marked into the system.

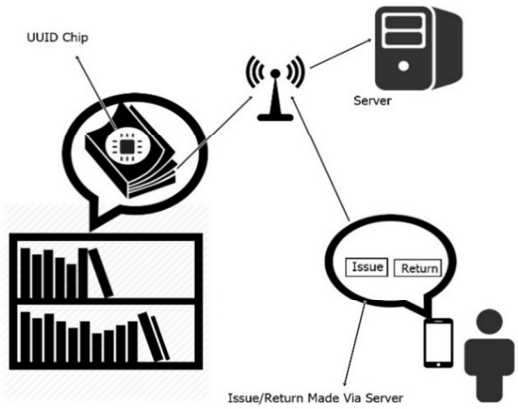
For students, along with their biometric credentials, their specialization and timetable will also be uploaded on the server. There will be smart sensors in the doors of the each class room. Sensors will detect the movement and smart doors will open automatically when anybody will stand in front of the door and close afterwards. The door will scan the person entering the classroom and will match its identity with the data stored in the database. Once the person is identified, the system will mark the presence of that student in that particular class. Students, teachers and administrative staff, all will have the access to view the attendance record of the students.

(iii) Smart Boards and Display



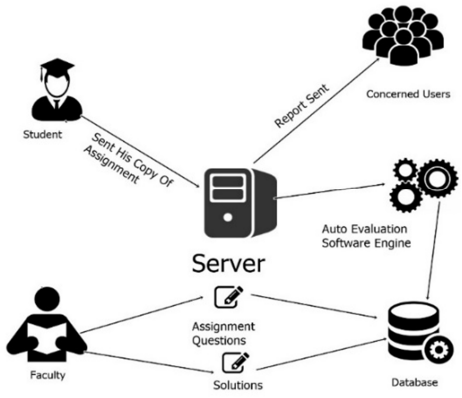
With the upcoming technology, the existing white boards will be replaced by smart boards. These boards will be equipped with live video streaming, writing and live communicating feature which will be controlled by using the multi touch enabled user screen which will scan the faculty and acquire the resources uploaded in advance by the faculty on the server. So, the faculty will automatically get access to his/her account. With this, the faculty, will be able to provide the students the information already uploaded on server or available online on a specific topic with interactive 5d video technology.

(iv) Smart Library



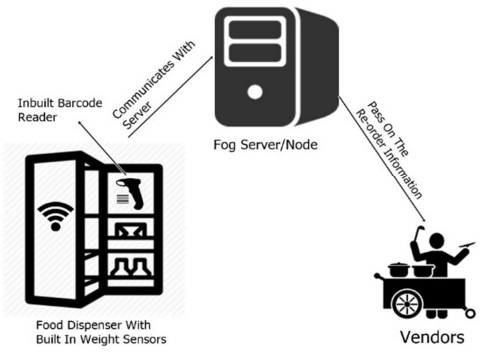
Libraries powered by IoT will be known as "Smart Libraries". In this, each book will have a chip which will contain unique id, title of the book, author, publisher etc. Doors of the library will open only after biometric authentication. Each person has to do biometric authentication for entering and exiting the library. These modern libraries will have sensors, when a student or faculty will take a book and move out of the Library, sensors on the doors of the library will read the book information from the chip and persons information from his/her biometric. The book will then be issued to that person. With delay in return of the book by the student, the system will automatically calculate the fine and send the details to accounts department of the Institute. To return the book, the person will just have to place the book on the desired slot or shelf. The sensors will identify the book and will automatically update the status as *book returned* in the database.

(v) Auto Evaluation



Online assignments will be given to the students. The system will not only check the submission status of the assignment but also check the plagiarism of the assignments and also evaluate and grade the assignments using the keywords and sample solution fed by the faculty into the servers.

(vi) Smart Canteen



The daily inventory will be recorded by the automatic system under smart canteens. The system will regularly check the inventory using barcodes on the food items. When the inventory of a particular item will reach below the minimum identified level, a re-order for the same will be placed automatically.

III. Security Issues in Smart Institutions

IoT is still work in progress. There are some limitations in implementation of IoT and is prone to multiple security threats. Some of these threats are:

- **Data Confidentiality**
  IoT processes a lot of data. Data retrieval and processing is the most concerned area of IoT environment, where 90% of the data is users' private data and should be kept confidential.

- **Data Authentication**
  There is no way to authenticate the data being transmitted from an IoT device, so the security is compromised. For example, we have appliances connected with controlling component in smart classes, there is no way to authenticate the data source and anyone can fake the device into thinking people are present in the room or vice versa. Authentication issues are looking small but have a huge security risk.

- **Side Channel Attacks**
  A side-channel attack is based on the information retrieved from the physical implementation of cryptosystem. This is due to brute force attack or weakness in the algorithms. Encryption and decryption algorithms always left with chances of side channel attacks. These attacks focus on how the information is presented rather than on the information itself. For example, vehicles' number plates data, camera footages and facial data can be accessed by side channel attacks.

- **Perceptions**
  With introduction of IoT, many users are concerned about their data privacy and having fear that their data might get stolen from their smart appliances. With the concerned level of risks attached to IoT, many people will hesitate to purchase connected devices

- **Hacking**
  Researchers with a motive to test IoT systems become able to hack connected devices. This leads to a possibility that the hackers could also replicate the same and hack these devices as well.

- **Unwanted Public Profile**

While using the connected devices from specific manufacturers users accept their terms of service. Most companies stated a term and condition that they will collect and offer the user's data to other companies for their own use like collecting the data related to driving habits from connected vehicles and share it with insurance companies to calculate user specific annual insurance premium.

- **Eavesdropping**
  With IoT, huge amount of data flows and it becomes easy for the intruder to eavesdrop the data. In this way, hackers can eavesdrop the data transmitted between connected device and can trespass a user's privacy.

IV. Conclusion

With the flow of time, technology is spreading more deeply into human lives. Technology has changed our lifestyle whether it is a smartphone in our pockets or a smart watch on our wrist or a fully automated smart home. IoT is still in its beta testing stage. It has its own flaws like data insecurities and exploitation because of unencrypted data flow. To overcome the limitations of IoT, continuous researches are going on all over the world. This digital transformation will reveal new insights that promise to change the future educational institutes and system. So, we can say that IoT will revolutionize the world and we will finally become one step closer to that educational institutes we think of from ages.

References

[1]. Alsaadi, Tubaishat, E. (2015). Internet of Things: Features, Challenges, and Vulnerabilities. *International Journal of Advanced Computer Science and Information Technology*.

[2]. Bandyopadhyay, Sen, D. (2011). Internet of Things - Applications and Challenges in Technology and Standardization, *International Journal of Wireless Personal Communication*.

[3]. Bonomi, F. (2013). The Smart and Connected Vehicle and the Internet of Things. *Cisco*. Available at https://tf.nist.gov/seminars/WSTS/PDFs/1-0_Cisco_FBonomi_ConnectedVehicles.pdf

[4]. Bonomi, Milito, Zhu, Addepalli, F. (2012). Fog Computing and Its Role in the Internet of Things. *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*

[5]. Ghanam, Ferreira, Maurer, Y. (2012). Emerging Issues & Challenges in Cloud Computing— A Hybrid Approach. *Journal of Software Engineering and Applications*.

[6]. Khatoon, M. (2014). FOG Computing and Its Role in Internet. *International Journal & Magazine of Engineering, Technology, Management and Research.*

[7]. Kumar, Goudar, S. (2012). Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. *International Journal of Future Computer and Communication*.

[8]. Lindsay, Woods, Corman, G. (2016). Smart Homes and the Internet of Things. *Atlantic Council*.

[9]. Niranjanamurthy, M., Kavitha, P.B., Kasana, P., Vishnu, S., N. ,. (2016). Research Study on Fog Computing for Secure Data Security. *International Journal of Science Technology and Management*.

[10]. More, P. (2015). Review of Implementing Fog Computing. *International Journal of Research in Engineering and Technology*.

[11]. Patil , P. V. (2015). Fog Computing. *International Journal of Computer Applications (0975 – 8887).*

[12]. Saharan, Kumar, K. (2015). Fog in Comparison to Cloud: A Survey. *International Journal of Computer Applications (0975 – 8887).*

[13]. Stojmenovic, Wen, I. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. *Federated Conference on Computer Science and Information Systems.*

[14]. Thierer, A. (2014). The Internet of Things and Wearable Technology. *Mercatus Working Paper*. Available at https://www.mercatus.org/system/files/Thierer-Wearable-Tech.pdf

[15]. Vaquero, Merino, L. M. (2014). Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing. *ACM SIGCOMM Computer Communication Review*.

[16]. Vouk, M. A. (2008). Cloud Computing – Issues, Research and Implementations. *Journal of Computing and Information Technology*.

[17]. Zanella, Vangelista, A. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*.

[18]. Sicari et.al (2015). Security, Privacy and Trust in Internet of Things: The Road Ahead. *Computer Networks, Elsevier publications.*