Analysing Space Utilization using Indoor Localization

Joy Aneja

IIIT-D-MTech-CS-14010

Indraprastha Institute of Information Technology, New Delhi

Thesis Committee
Dr. Pushpendra Singh (Chair), IIIT Delhi
Dr. Viswanath Gunturi, IIIT Delhi
Dr. Debopam Acharya, SNU

Submitted in partial fulfillment of the requirements
for the Degree of M.Tech. in Computer Science

All rights reserved

Keywords: Wireless Local Area Network, Simple network Management Protocol, SNMP Traps

Certificate

This is to certify that the thesis titled **Analysing Space Utilization using Indoor Localization** submitted by **Joy Aneja** for the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science & Engineering is a record of the bonafide work carried out by him under my guidance and supervision at Indraprastha Institute of Information Technology, Delhi. This work has not been submitted anywhere else for the reward of any other degree.

Dr. Pushpendra Singh
Indraprastha Institute of Information Technology, New Delhi

Abstract

The wide deployment of IEEE 802.11 Wireless LAN in offices, colleges and other organizations makes it a prime solution for indoor localization. Wireless access point awareness and its small cell size helps in localizing network devices. It is a cost efficient solution as it works with the existing infrastructure and does not require any specialized hardware deployments. Wide deployment of indoor localization and without any direct involvement of users enables it for various applications and services like space utilization, power conservation etc. This work analyzes SNMP traps sent by the access points to the NMS and determines the symbolic location of the network devices and exposes this real-time information through a robust, flexible and loosely coupled platform. This platform is enabled to analyze space utilization which is important in higher education institutions as a balance has to be maintained between minimizing costs and meeting pedagogical and research needs of professors, and the learning and support needs of students. Further, this work also deploys some applications like personalized timelines, time spent and others.

Acknowledgements

This dissertation would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this work. First and foremost, I would like to thank my supervisor, Dr. Pushpendra Singh, for his guidance and encouragement throughout the course of my study at IIIT Delhi. I am deeply indebted to him for inspiring me to work hard at all times. I would also like to thank my friend Digvijay Singh, who helped me understand the existing infrastructure.

My parents are my source of inspiration and this thesis would have been incomplete without their support. It is their endurance that kept me motivated at all times. Finally, I would like to thank all my friends, especially Amandeep, Pradyumn, and Yash for making my stay at IIIT Delhi, a pleasurable experience.

Contents

List of Figures

Chapter 1

Introduction

1.1 Localization

Localization refers to the process of determining an object's location in space. Although it is considered to be a modern technology but it has been in use centuries back. Many primitive localization methods exist, which do not require any use of special instruments and were being used for maritime navigation by sailors. Since the early dawn of European medieval age, they have been using motion of celestial bodies, the position of certain wildlife species, or size of waves to find their location and path to another island. Since then, many specialized tools have been invented for determining position more accurately by reducing the error of distance from the actual position, most notably astrolabe, sextant, compass, and chronometer with detailed maritime charts and maps. Use of high range radio signal transmitters fitted on lighthouses present on the shores was first seen in late 1920s. During 1960s, the United States Department of Defence (DoD) began developing a satellite-based localization system for military purposes, which eventually evolved into Global Positioning System (GPS) [1].

However, GPS had started to delve into public sector from as far back as 1983 but to discourage proliferation of these devices, DoD activated Selective Availability (SA), a purposeful degradation in the GPS signal intended for civilian usage, which limited the accuracy of these units to about 100 meters. Finally in the year 2000, the DoD decided to turn off the degradation of signals for civilian usage in view of increasingly important role played by GPS in number of commercial activities. Later, large number of research started on GPS systems which resulted in increase in an accuracy of up to 10 meters or better. With the advent of Differential GPS, the accuracy of centimeter level is achievable but only in case of best implementations [2].

However, GPS signals are attenuated and scattered by roofs, walls, human bodies, and other objects. Hence, they are usually badly degraded or completely unavailable in environments such as cities, urban canyons and especially indoors essentially all of the places where most people live, work and play. Therefore, Localization is mainly classified into indoor localization and outdoor localization. Outdoor localization deals with the problem of localization in an outdoor environment where there is no or limited obstruction of signals from satellite, hence there GPS works extremely well.

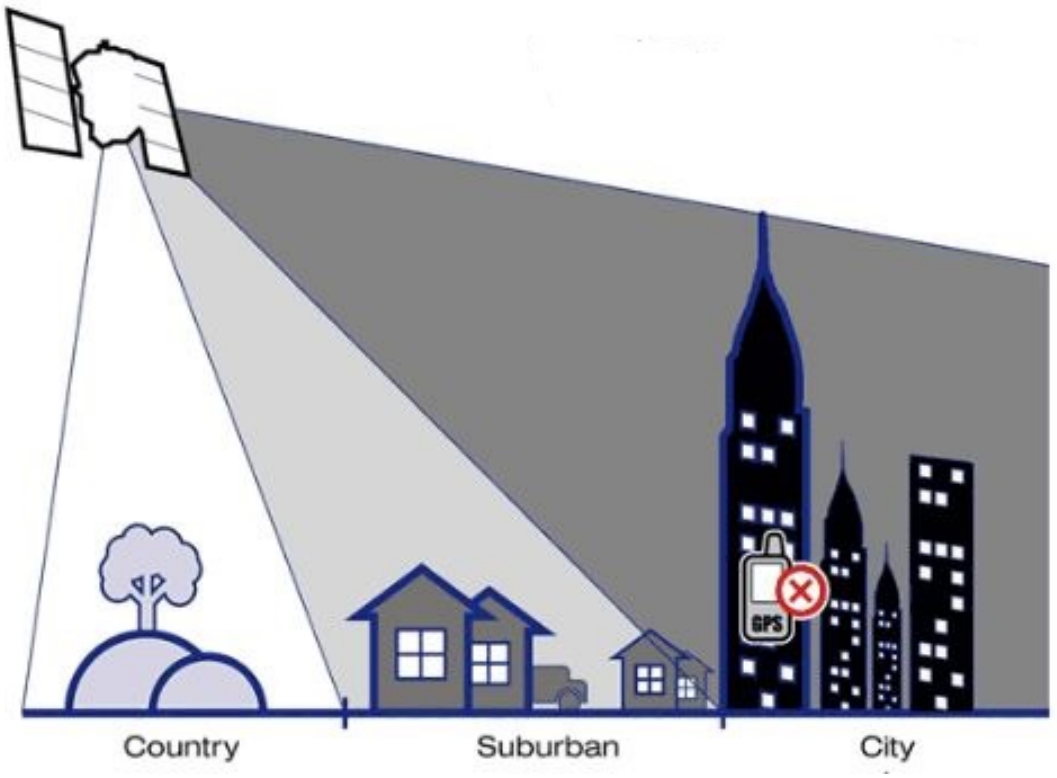

Figure 1.1: GPS signal strengths [9].

Indoor localization deals with the problem of localization within high-rises of a city, urban canyons and especially inside the house on some floor of a building. In this case, GPS fails miserably as the signals lose significant power indoors affecting the required coverage [3]. It is an active research problem. Liu et al. [3] and Hightower et al. [4] proposes solutions for indoor localization, but all these solutions require some extra hardware deployments either in form of towers with transceivers like in Locata [9], or they require small transceivers distributed among the people like in SpotON [10] which uses active RFID technology. These solutions require large amount of financial investment and distribution of capable devices to everybody. Other solutions like of Otsasen et al. [5] which proposes use of GSM/CDMA technology or of Bahl et al. [6], Ladd et al. [7][8] which proposes use of wireless local area network (WLAN), they require large amount of fingerprinting and still will not give similar results for a wide variety of cellular or Wi-Fi devices. These solutions also require reporting software on these devices by which they report to the server about their signal strengths, which use power and space on individual devices, and everybody may not be willing for it.

1.2 Space Utilization

Space utilization is a measure of whether and how a valuable commodity known as space is being used [11]. Space Utilization is a strategically important space management measure for any type of organization. It can help organizations to assess what size of estate is affordable by calculating the cost of having the estate and this is kept fit for purpose and in good condition. Utilization studies provide information on how

the space is being used and help to inform decisions about the type and scale of facilities needed. These studies raise questions about the most effective use of resources which are available. If some space is not being used, is it needed and does it need to be funded? Could the resources consumed by under-used space be better directed elsewhere?

In the case of higher education institutions, analysis of space utilization becomes of utmost importance as there should always be a balance between minimising costs, meeting pedagogical and research needs of staff, and the learning and support needs of students. Effective utilization of space also creates a good match between space needs and space provision and helps to improve the staff and student experience.

While new construction is nice and growing number of buildings are often viewed as legacy accomplishments, the reality is that each new building adds to campus carbon footprint [13]. Colleges and universities can save money and reduce carbon emissions by maximizing the utilization of existing space and avoiding new construction altogether. Usually, the most desirable spaces may be intensively utilized and fought over while less desirable spaces are cast off and sparsely occupied. Over time, as new buildings are constructed and departments and offices move into those glitzy, high prestige spaces, the areas they leave behind are taken over by existing personnel and offices, which has net effect of decreasing space utilization density. Ever greater areas are used while activity and output stays roughly the same.

1.3 Problem Definition

Analysing space utilization has been a long-existing and challenging problem. The focus of this work is to deploy a system for indoor localization and use it to analyse space utilization in the campus of IIIT-Delhi. Indoor localization is implemented using the technique mentioned by Chen et al. in which he suggests the use of SNMP traps for localization of Wi-Fi enabled devices [15]. It is assumed that most of the occupants carry a Wi-Fi enabled device like a mobile phone with them as Mark Weiser had correctly predicted in computer for 21st century [14]. This indoor localization method gives an accuracy of 10-12 meters and can be widely deployed without direct involvement of the occupants. It gives us the symbolic location of the individual which can be classified using labels such as floors, buildings etc. This system is then employed to analyse space utilization of the campus. This enables to give insights into which spaces are underutilized and where work actually happens. Further, it allows to identify ways to improve space utilization and increase efficiency, usually resulting in significant maintenance cost savings. This analysis enables us to further develop strategies to improve staff, students and guests satisfaction and productivity based on their spatial needs. It allows managers and admins to align spatial needs to meet overall organizational goals and objectives.

The system also enables the development of applications which solve real world problems applications. As a part of this work, applications have been deployed like schedule logging which displays the schedule of an individual where and how much time has he spent, time spent which presents the amount of time is spent at a particular loca-

tion, and presence calendar to mark your days at some location. Additionally, more applications can be built over this system which can range from solving problems in organizational space [16], spatial sciences [17] etc. to study of visitor behaviour, campus walkthrough for visitors [18], HVAC control [19], and trigger context aware information services.

1.4 Outline

This dissertation gives a clear view of the research done. It has been divided into several chapters. In the first chapter, we introduce localization, space utilization and how space utilization can be achieved by first conglomerating the occupancy data and then analysing to get insights. In the second chapter, existing infrastructure of wireless LAN and SNMP are discussed which are key components in our system. In the third chapter, we discuss the design and architecture of the system by which we achieve the requirements of the system. In the fourth chapter, we discuss space utilization techniques which haven enabled by the system. In the last chapter, we give the categorical future scope and conclusion to our dissertation.

Chapter 2

Preliminaries

The deployed system uses the existing Wireless Local Area Network (WLAN) in the campus of IIIT Delhi. It utilizes the Simple Network Management Protocol (SNMP) to collect current and accurate occupancy data from the network.

2.1 Wireless Local Area Network (WLAN)

A WLAN is a wireless computer network that interconnects many devices using a wireless distribution method within a limited area. Most WLANs are based on IEEE 802.11 standards [25]. All components that can connect into a wireless medium in a network are referred to as stations. All stations are equipped with wireless network interface controllers. These wireless stations can mainly be divided into two main categories namely, wireless access points and mobile or wireless clients. Access points are base stations for the wireless network and are normally wireless routers. Wireless clients can be mobile devices such as smart-phones, laptops, personal digital assistants (PDAs), or other fixed devices such as desktops and workstations that are equipped with a wireless network interface cards.

The IEEE 802.11 has two basic modes of operation namely, *infrastructure* and *ad-hoc mode*. In ad-hoc mode, mobile units transmits directly peer-to-peer, while in infrastructure mode, mobile units communicate through an access point that serves as a bridge to internet or LAN. Most of the Wi-Fi networks are deployed in infrastructure mode. In this mode, all mobile and wireless client devices and computers communicate with the access point (AP), which provides the connection from the wireless radio frequency network to the hard-wired LAN. If the access point is connected to a LAN, it performs the conversion of IEEE 802.11 packets to IEEE 802.3 Ethernet LAN packets. Data packets travelling from the LAN to a wireless client are converted by the access point into radio signals and transmitted out. All the mobile and wireless clients or devices receive the packets, but only those clients with desired destination address will acknowledge and process the packets.

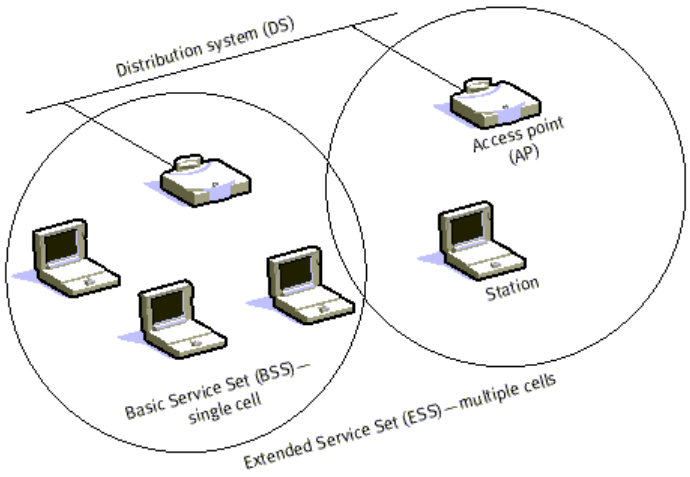

Figure 2.1: Extended Service Set (ESS).

A basic wireless infrastructure with a single access point is called a Basic Service Set (BSS). When more than one access point is connected to a network to form a single sub-network, it is called an Extended Service Set (ESS). Access points in ESS are interconnected by a distribution system. Each ESS has an ID called the SSID which is character string with a maximum size of 32 bytes. A distribution system is used to increase network coverage through roaming between cells. It can be wired or wireless. Current wireless distribution systems are mostly based on Wireless Distribution System (WDS) or MESH protocols [26] [27]. Most big organizations like universities, offices, etc. have campus wide Wi-Fi networks which are possible only due to ESS. They situate hundreds of interconnected APs within their buildings for seamless internet connectivity.

The 802.11 specification includes roaming capabilities that allow a client computer to roam among multiple access points on different channels. When a Mobile Station (MS) moves from one access point to another access point within a home network because the signal strength is too weak it is called internal roaming or handoff [28]. A MS roaming from one access point to another often interrupts the flow of data among the MS and application connected to the network.

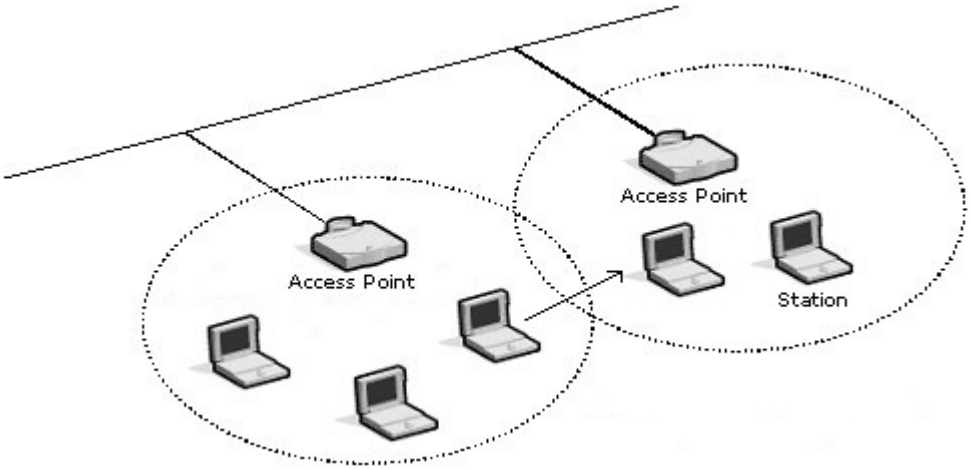

Figure 2.2: Handoff process.

The handoff process involves a sequence of messages being exchanged between the MS and the participating access points. The process can be divided into discovery phase and re-authentication phase. In discovery phase, when the MS is moving away from an access point, the signal strength and signal-to-noise ratio decrease, which causes MS to initiate a handoff. A MS periodically monitors the presence of alternative access points which provide better signal strengths and signal-to-noise ratio. In re-authentication phase, the MS authenticates itself and then after successful authentication, it re-associates itself with the new access point. However, the MS may lose a connection with an access point before associating with another access point.

2.2 Simple Network Management Protocol

SNMP is an internet standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour. It exposes management data in the form of variables on the managed systems, which describe the system configuration [20].

An SNMP managed network consists of three key components.

- Managed Device
- Agent
- Network Management Station (NMS)

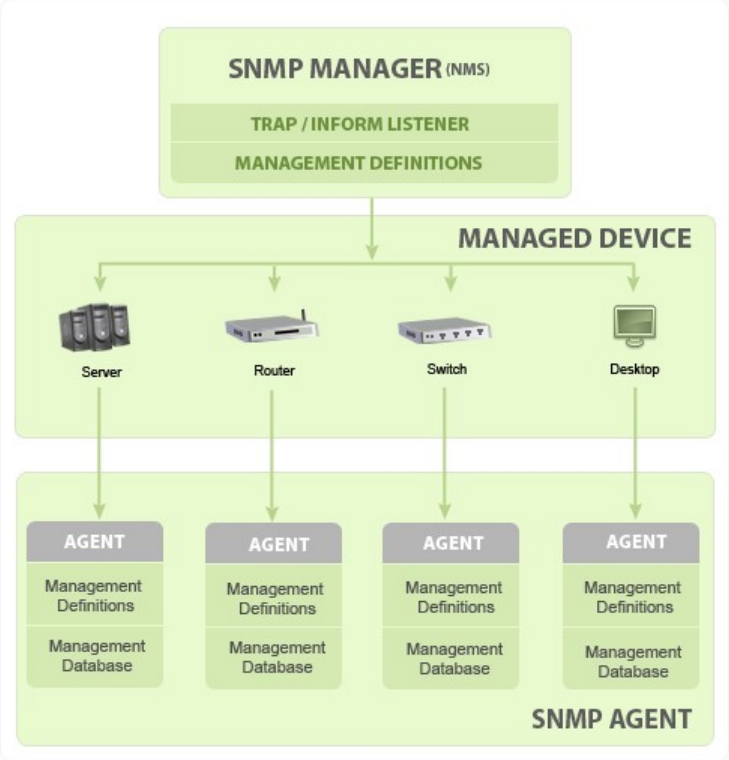

Figure 2.3: Components of SNMP [39] .

Managed Device - It is network node that allows unidirectional or bidirectional access to node-specific information and implements SNMP interface. They can be of any type viz. routers, access server, switches etc.

Agent - It is network management software module that resides on managed device. It collects the management information database from the device locally and makes it available to the SNMP Manager, when it is queried for. These agents could be standard like Net-SNMP or specific to a vendor like HP insight agent.

Network Management Station (NMS) - It executes applications that monitor and control managed devices.

Every SNMP Agent maintains an information database describing the managed device parameters or variables. The SNMP manger uses this database to request the agent for specific information and further translates the information as needed for the NMS. This commonly shared database between the agent and the manager is known as Management Information Base (MIB) or Management Information Database. This database is of hierarchical structure and each entry is called managed object, which are addressed through an Object Identifier (OID). Each identifier is unique and denotes specific characteristics (or variable) of a managed device. These variables can be of different data types like text, number, counter etc. There are two types of managed objects viz. Scalar and Entity Table [21]. Scalar managed objects contain only one value while Entity Table managed object can contain multiple values in the form of table. Devices vendor name is an example of scalar and CPU utilization is of type

entity table, as in case of quad processor there would be a result for each processor. A typical OID is a dotted list of integers for instance OID for sysDesc is 1.3.6.1.2.1.1.1 in RFC1213. In this representation, every integer corresponds to a hierarchy level. It can also be represented textually as *iso.identified-organization.dod.internet.mgmt.mib-2.system* which is defined in ASN.1 [22].

Basic commands in SNMP

The simplicity in information exchange has made the SNMP as widely accepted protocol. The main reason being concise set of commands.

- GET: This operation is used to retrieve one or more values from the managed device by the manager.
- GET NEXT: This operation is similar to GET, but it retrieves the value of the next OID.
- GET BULK: This operation is used to retrieve large number of variables.
- SET: This operation is used by the managers to modify or assign the value of some variable.
- TRAP: Unlike the above commands which are initiated from the SNMP manager, traps are initiated by the agent. It is a signal to the SNMP manager by the agent on occurrence of an event.
- INFORM: This command is similar to TRAP, but it also includes confirmation from the SNMP manager on successfully receiving the message.
- RESPONSE: This command is used to carry back the value(s) of actions directed by the SNMP manager.

SNMP Traps

SNMPv1 and SNMPv2 encourage trap-directed notification[23]. To reason this, lets assume a manager is responsible for a large number of devices, and each device has a large number of objects, if a manager keeps on polling or requesting information from every object on every device, it will lead to substantial traffic of frivolous SNMP request and responses. This can be avoided by using trap-directed notification, in which each agent on the managed device has to notify the manager without solicitation about any change in its objects. This results in substantial savings of network and agent resources.

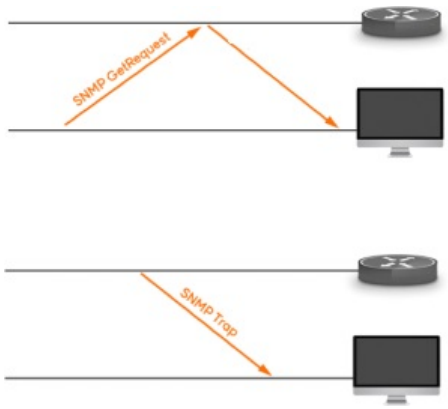

Figure 2.4: GET request and response versus SNMP trap.

In order for the manager to understand these traps, data is encoded in the key-value pair configuration. These pairs are called variable bindings and they contain extra information relating to the trap. For instance, an SNMP trap might contain variable bindings for *domain name, urgency level, and alert description.*

SNMP Trap Communication

SNMP traps are sent to NMS whenever there is a change in any of the variables at the managed device or if there is any alert from the managed device. Initially, the trap is generated by the SNMP Agent using Management Definitions and Management Database, which is then packed in UDP Datagram and sent to NMS. Figure 2.5 shows the steps in which trap is transferred to NMS. In infrastructure wireless LAN with ESS, whenever a managed device moves from one access point to another, it generates a series of SNMP traps which are sent to the NMS. These traps will be discussed in the next chapter.

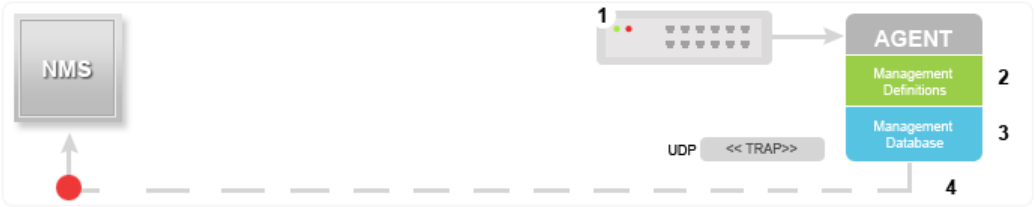

Figure 2.5: SNMP trap communication [39].

The SNMP messages are generally transferred using User Datagram Protocol (UDP) and not Transmission Control Protocol (TCP) by default, this is because the network management must be robust and also work under heavy congestion and TCP requires a certain critical threshold to work while UDP can work in well below reliability than TCP threshold [24].

Chapter 3

System Design

The system is real time software which collates and processes the data received from the NMS as well as provides access to this information for analysis and finding useful insights from the data. This system has been deployed at IIIT Delhi which has 8 major blocks namely, Academic building, Library building, Lecture block, Dining building, Girls Hostel, Boys Hostel, Service Block, and Faculty Residence. Wi-Fi is accessible in all these blocks which helps in indoor localization. Adequate number of access points are installed on all floors of these blocks. The access points along with the whole network is managed by a dedicated IT Operations team. The access points are placed in an optimum way and are labeled according to their symbolic location.

3.1 Design Goals

The system is designed to cater the end user's requirement of robust and real-time information about indoor localization and space utilization. While designing of the system these goals have been kept in mind:

- A robust and real-time platform to give access to the localization information.
- A secure, scalable[1], elastic[2] and schema-free[3] data storage to enable growth of the system to accommodate new sources.
- An abstract design to enable development of applications independently of complexity of the core system.
- An easy-to-use, robust, flexible and loosely coupled web application for end user.

3.2 External Dependencies

The system exists in between an infrastructure of external dependencies like wireless network and NMS. This section gives an overview of the whole infrastructure required. It takes the system as a black box, and defines as well as describes its external dependencies.

[1] Capability to grow in size, or process to handle a growing amount of work
[2]Flexibility of its data model
[3]Ability to modify its schema without any downtime

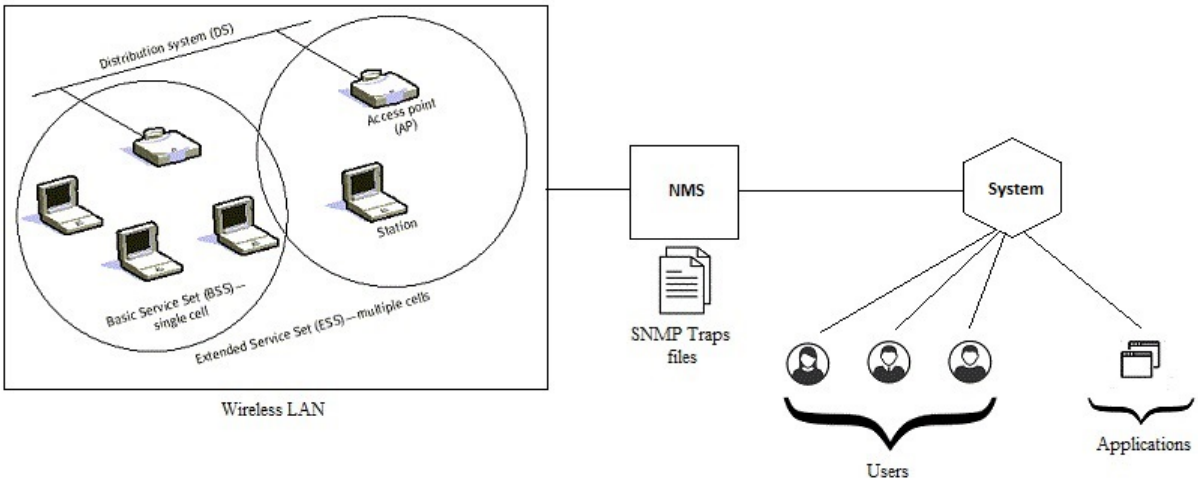

Figure 3.1: External dependencies of the system.

Wireless LAN

It includes all the devices which are connected to the wireless network. These devices can be wireless and mobile like smart-phones, laptops, tablets or any other devices with wireless connectivity. These devices get connected to the nearest or most optimum access point from which they have better signal strength and signal-to-noise ratio. These access point have associated with them their symbolic locations and hence from this connected devices' symbolic location can be inferred.

It is not necessary that a device or station is connected to its nearest access point at some particular time, this may be because of attenuation of Wi-Fi signals from the nearest access point, or if a device is coming from a range of another access point, it does not tend to disconnect from the previous access point until a very low threshold of signal strength as the handoff process requires more time and power. But usually it is assumed, that if there is a change in floor, the device changes it access point to a new access point on that floor as change in floor causes high attenuation due to concrete slab and metal rods in between and hence reduces the signal strength and signal-to-noise ratio. This work considers the block name and floor as the highest level of precision for symbolic location. Improvement in level of precision is kept as a future scope of this work.

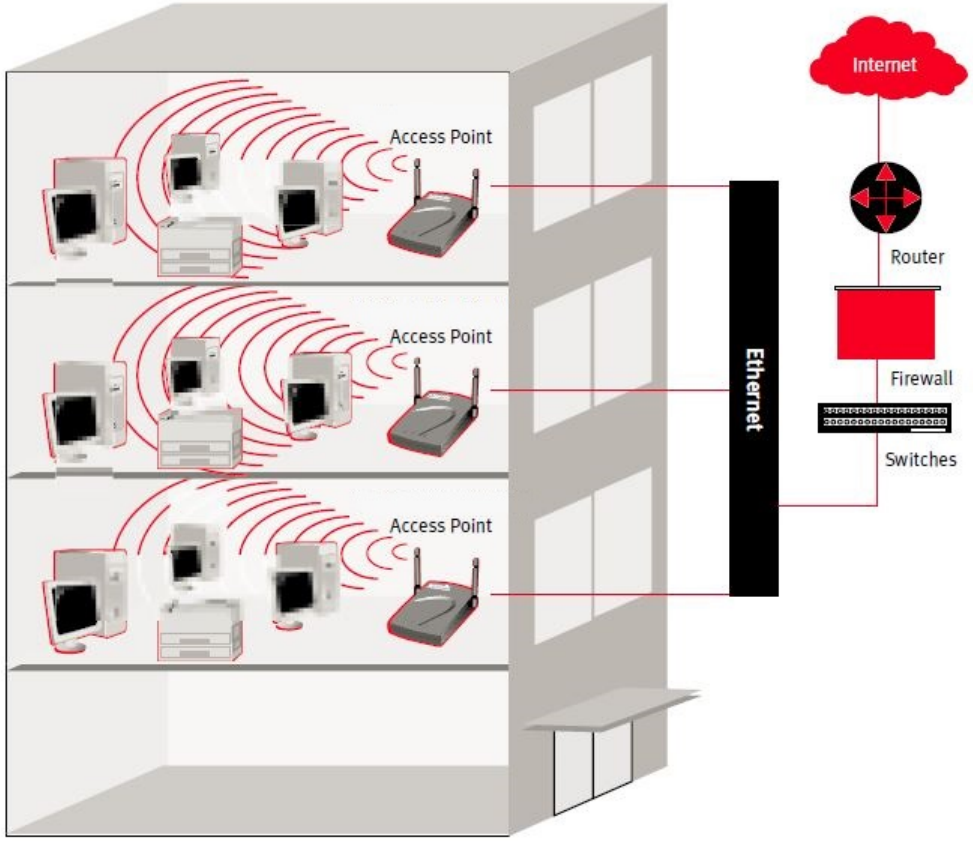

Figure 3.2: Distribution of access points on floors of a building. [40]

Whenever a device or a station connects to an access point, the SNMP agent generates a SNMP trap which is sent to the NMS.

Network Management Station (NMS)

A NMS is a server that runs a network management application. Network elements communicate with the NMS to relay management and control information. SNMP is used to communicate management information between the network management stations and the agents in the network elements. SNMP traps which are sent to NMS are written in files for storage. SNMP traps can be of many types like association, disassociation, faults, etc. Net-SNMP is a suite of software for using and deploying the SNMP protocol. It is used for receiving asynchronous traps generated by the system. It is configured to log these traps into a file on the NMS. Some type of traps which are important to this work are discussed below.

1. ciscoLwappDot11ClientMovedToRunState
   Cause: A client has completed a security policy.
   Description: A client has completed all the formalities of connecting to an access point and have been assigned the IP address to send or receive data. It

is now in running state [31] [32].
Trap Components:

- Client's MAC Address
- Access point's name or label
- Access point's MAC address
- Client IP address
- Client's connected SSID

2. bsnDot11StationAssociate
Cause: A client has associated with an access point.
Description: The associate notification shall be sent when any of the watch listed client (present on at least one watch list) associates with an access point [31] [32].
Trap Components:

- Access point's MAC address
- Client's IP address
- Client's MAC address
- Access point's name or label

3. bsnDot11StationDeauthenticate
Cause: A client is no longer authenticated by the system.
Description: The deauthenticate notification shall be sent when the station sends an deauthentication frame [31] [32].
Trap Components:

- Access point's MAC address
- Client's IP address
- Client's MAC address
- Access point's name or label
- Reason for deauthentication

4. bsnDot11StationDisassociate
Cause: A station or device might disassociate due to various reasons such as inactivity time-out or a forced action from the management interface.
Description: The disassociate notification shall be sent when the station or device sends a disassociation frame [31] [32].
Trap Components:

- Access point's MAC address
- Client's IP address
- Client's MAC address
- Access point's name or label
- Reason for disassociation

5. ciscoLwappDot11ClientCoverageHolePreAlarm
   Cause: Data coverage hole detected.
   Description: This notification is generated when the access point receives at least 'packet count' packets for voice or data, from a client in any given 5 second interval and 'packet percent' of the packets, from the client are below the 'RSSI threshold' [32].
   Trap Components:

   - Access point's MAC address
   - Client's IP address
   - Client's MAC address
   - Access point's name or label
   - Access point's transmit power level
   - Transmit timestamp
   - Comma separated histogram values
   - Neighbour access point's MAC address
   - Neighbour access point's RSSI

6. ciscoLwappDot11ClientDisassocDataStatsTrap
   Cause: A client is no longer associated to the system.
   Description: Data statistics of the client after it has been disassociated from the system [33].
   Trap Components:

   - Access point's MAC address
   - Client's IP address
   - Reason for disassociation
   - Client's connected SSID
   - Client's Session ID
   - Client's transmitted data packets and bytes
   - Client's received data packets and bytes

7. ciscoLwappDot11ClientAssocDataStatsTrap
   Cause: A client has associated with an access point.
   Description: Initialised data statistics of the client [33].
   Trap Components:

   - Access point's MAC address
   - Client's IP address
   - Reason for disassociation
   - Client's connected SSID
   - Client's Session ID
   - Client's transmitted data packets and bytes

- Client's received data packets and bytes

8. ciscoLwappDot11ClientSessionTrap
   Cause: A client has completed the Policy Enforcement Module (PEM) state and movies to running state.
   Description: A client is associated with an access point and is issued a session ID [33].
   Trap Components:

   - Access point's MAC address
   - Client's IP address
   - Access point's name or label
   - Client's connected SSID
   - Client's Session ID

There are more types of traps which are generated by the devices, but they are not important for this work and hence have been omitted. These traps are written to a file stored on NMS. The rate of incoming of these traps can range from 4 traps per second to 16 traps per second.

System, Users and Applications

These traps which are written onto a file in NMS are read by the system by creating a SSH connection to the NMS and using *tail f* to read the traps. These traps are then stored in the database at real-time. Users and applications can access the data from the database without any significant delay (¡ 1s) from the actual time of trap writing. The full white box architecture of the system is explained in the section 3.4.

3.3 Tools and Technologies

The system has been developed using Spring web framework and using a NoSQL database MongoDB for the data storage.

Why Spring?

- Spring enables to develop the enterprise applications using POJOs (Plain Old Java Object). The benefit of developing the applications using POJO is, that we do not need an enterprise container such as an application server but we have the option of using a robust servlet container.
- Inversion of Control (IOC) container: This provides a loose coupling between the objects in the system, simplifying connections between the modules.
- Aspect Oriented Programming (AOP): It supports AOP that enables convenient development by separating application business logic from system services.

- JDBC Abstraction framework: it simplifies implementing the DAOs using JDBC by providing built-in solution for problems like code duplication, resource handling and exception handling. For instance, it can convert the SQLException into meaningful exception hierarchy simplifying the error handling strategy.

Why NoSQL?

- Flexible Data Model: NoSQL databases address the requirements for the data that is semi-structured or unstructured in nature. Document, graph, key-value or wide-column, all of them offer a flexible data model, making it easier to store and combine data of any structure and allow dynamic modification of the schema without downtime.
- Elastic Scalability: These databases include support for sharding or partitioning, allowing the database to scale-out for almost unlimited growth.
- High Performance: These databases are designed to deliver great performance, measured in terms of both throughput and latency at any scale.

Why MongoDB?

- Document oriented database: Only one document is capable of storing all the information required for one trap. Fields of document can be allocated with any type of information including arrays and embedded documents. This allows documents to have a very rich and flexible structure.
- Schema-free: Schema design can be on-the-fly, leading to much faster development and upgradation.
- Scalability and load balancing: Automatic data movement across different shards for load balancing to maintain even distribution of data among all servers in a cluster.
- JSON: It uses JSON objects to store and transmit information. JSON is the web standard protocol.
- Huge performance in handling large amount of incoming traps.
- Indexes and full query language, allows for Map-Reduce using JavaScript functions at the server side.

3.4 Architecture

3.4.1 Hexagonal Architecture

The system has been designed using the principles of hexagonal architecture. The term Hexagonal Architecture also known as Ports & Adapters architecture, was first coined by Alistair Cockburn. This architectural model is an applicative-architecture-style that helps to focus on business goals without being tied or jeopardized by technical frameworks or infrastructure choices. It allows an application to equally be driven by users, programs, automated tests or batch scripts, and to be developed and tested in isolation from its eventual run-time devices and databases. It makes the application ignorant of the nature of the input device and when something is to be outputted, it sends it out through a port to an adapter, which creates an appropriate signals needed by the receiving technology. Similarly, as events arrive from external dependencies at a port, a technology-specific adapter converts it into a usable procedure call or message and passes it to the core domain. This makes the application have a semantically sound interaction with the adapters on all sides of it, without actually knowing the nature of the things on the other side of the adapters [30].

This architectural model is designed in a way to prevent the infiltration of business logic into the external dependencies' (like UI) code, as this infiltration leads to low maintainability and testability. The model defines two main areas - inside and outside. Inside consists of applicative use case handlers and business domain code, while outside consists of DB access, messaging and communications, bindings etc. This model espouses Dependency Inversion Principle (DIP), which states that high-level modules should not depend on low-level modules and both should depend on abstractions, as in this all the dependencies are always towards the inside [35].

Benefits of using hexagonal architecture

- Sustainability: It decouples the application-business code from the tools like libraries or frameworks.
- Adaptability: Adding a new tool or technology to interact with the system is very easy. It only requires to add a new port-adapter to support it.
- Understandability: it does not mixes the use cases with tools as use cases handlers are defined in a dedicated module.
- Testability: It eases the usage of mock dependencies like databases, in order to test the applicative services and domain code.
- Domain Driven Design (DDD) compliant: As it does not allow the domain code to be contaminated by the infrastructure code.

3.4.2 System Architecture

Figure 3.3 gives the system architecture and all its components. The system is divided into three main layers viz. Core Domain, Adapters, and Ports. In this, ports are

dependent on adapters and similarly, adapters are dependent on core domain. The dependencies are always towards the inside. The arrows in the diagram represents dependency. Flow of data in the system is important to understand before delving into the detailed. The system receives the traps data from the NMS by creating a SSH connection and then tailing the SNMP traps log file. This enables the system to receive it line-by-line, which is then collated to form a single trap. This trap is then passed onto the parsing module and privacy module, which parses it into domain objects after hashing the private information, and are stored in the database. The database is updated with the real-time data. This real-time data is immediately available from the database to all applications and users for access. Users and applications can access the data after valid authentication and authorization. The data can be fetched using REST APIs or through web applications.

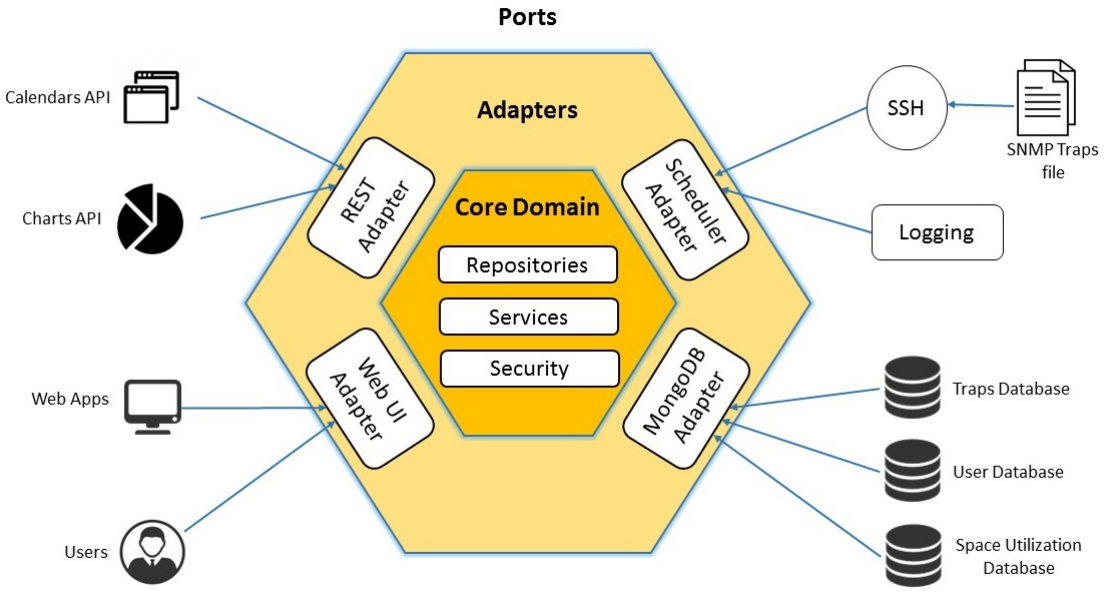

Figure 3.3: System architecture.

Now, moving onto the components, they can be thought of as the slices of the hexagon. Each component has a part of core domain, adapters, and ports. Although the dependency is towards inside, the interaction or communication can occur both ways. The ports can interact with core domain using the adapters or the core domain can interact with ports using technology-specific adapters. The goal of describing the architecture in components is to make conceptual divisions across functional areas of an application. The components will be discussed in subsequent sections.

REpresentational State Transfer (REST) Component

This component enables the interaction between the different APIs like Chart API or Calendar API (ports), controllers (adapters), and REST domain or entities (core). Events or clients request come at the port and the technology-specific adapters convert

these requests into usable procedure calls or messages and passes to the business logic.

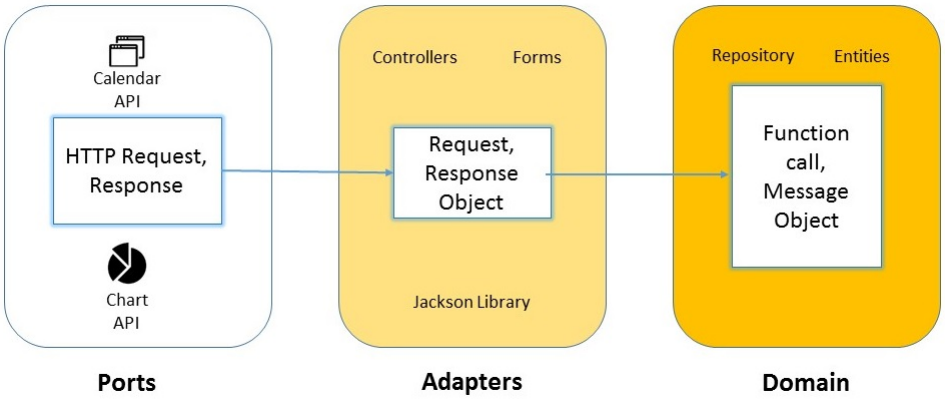

Figure 3.4: REST Component.

Charts API requests data for different types of charts like schedule charts, footfall charts, space utilization charts, etc. These HTTP requests (GET, POST) is converted to request objects by the respective controllers. These objects then call for messages from the business logic. These functions then return the data from the database in the form of DTOs (Data Transfer Objects). The DTOs are converted back to HTTP response using Jackson library to convert Plain Old Java Objects (POJO) to JavaScript Object Notation (JSON). The HTTP Response is sent back to the port. This JSON is then used as an input to the charting library.

Scheduler Component

This component enables the interaction between the different external services like SSH or logging (ports), scheduler (adapters), and repository or entities (core). Scheduled events or trap data come at the port and the technology-specific adapters convert these requests into usable procedure calls or messages and passes to the domain for service execution or data storage.

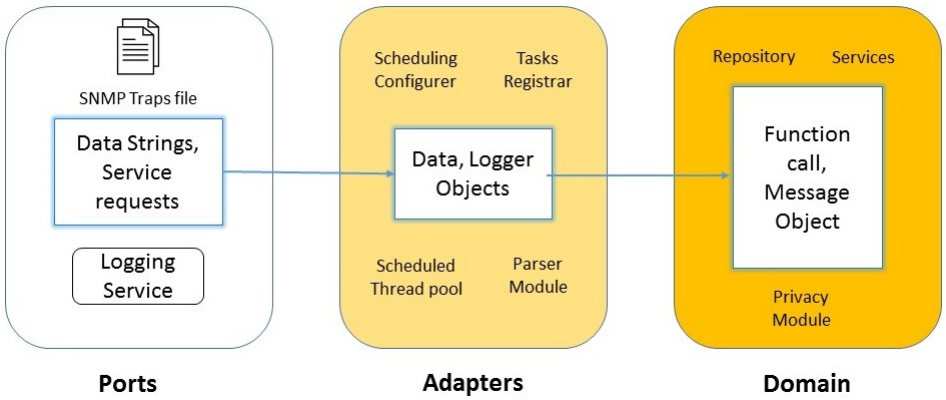

Figure 3.5: Scheduler Component.

Through the SSH connection to the NMS using the Java Secure Channel (JSch) library a tailing command (tail -f) is given to the traps log file. This command sends a line which is written onto the file to the system. All these lines are collated until an entire trap is formed. This trap is of textual form , which is then parsed into a domain object. Privacy module here hashes (SHA 256) the private information like MAC address, IP address or any other information that can trace back to the mobile device. This object is then send for storage. Logging service logs the time information of the traps which are being stored in the database. This service continuously runs in the background to log the current traps. This enables the admin to monitor and make sure that the trap parsing and storing remains real-time. Scheduled thread pool assigns the maximum number of threads which can be generated for different scheduled tasks. Currently, it is set to 200, but it can be increased as the number of tasks increases.

Database Component

This component enables the interaction between the different databases (ports), repository implementations (adapters), and repository or entities (core). Function calls for inserting or accessing data comes from the domain and the database-specific adapters (repository implementations) convert these requests into database queries and passes to the database at the ports.

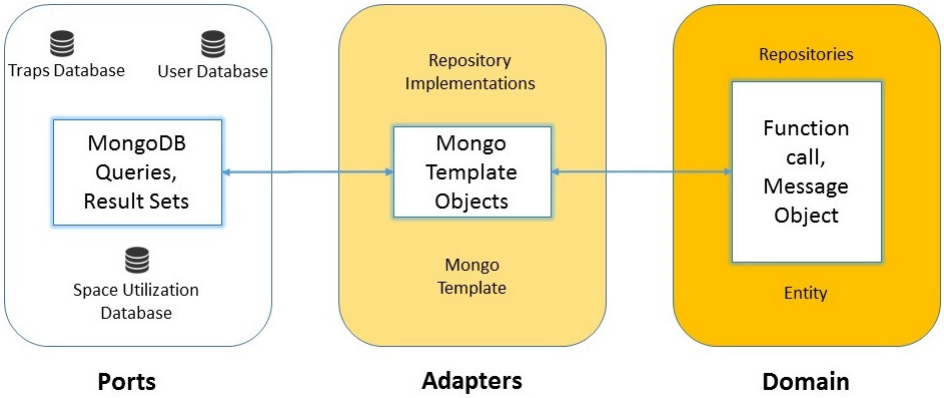

Figure 3.6: Database Component.

Whenever there is a requirement for data fetch, update or insertion, the functions which are declared in repositories are invoked. These functions are defined in the repositories implementations. These implementations convert the function call into a specific database query. These queries then return the data in the form of result sets. This data is converted back to DTOs by the adapter and then the DTOs are transferred back to the domain. Traps database is used for the storage of the received SNMP traps. This database is continuously being updated with new traps. It can be queried anytime for real-time data for MAC specific, location specific or time specific queries. Users database stores the account information of the users like email id and their stored hashed in a secure way. It adds a user whenever someone stores his MAC address for quick access. Space Utilization database stores the data about the usage of the location. It is updated with new data every midnight. The data schemas are

briefly described in Appendix A for reference.

Web UI Component

This component enables the interaction between the web applications and their users (ports), models and views (adapters), and repository, entities, authentication and authorization of users (core). HTTP requests comes from the ports for accessing the web pages for an application or authentication requests by the users and these are converted to function calls or messages for the controllers by the adapters. Then these functions call for services like authentication and authorization in the domain.

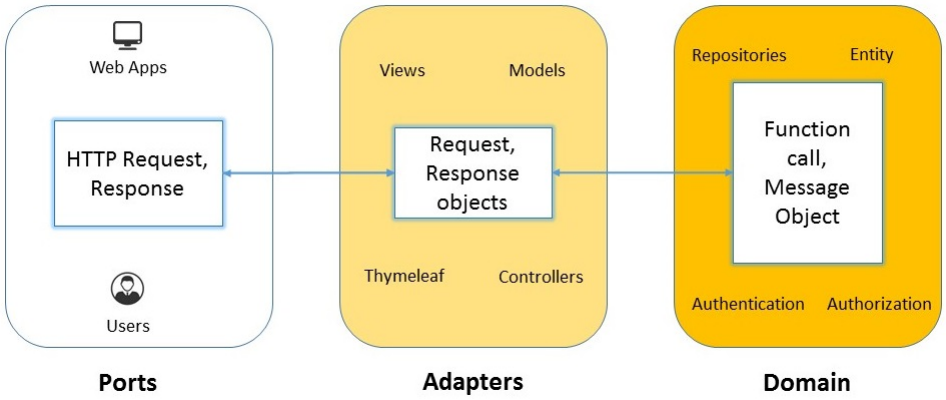

Figure 3.7: Web UI Component.

Authentication of users is done using the Google Identity Platform, after this authentication it is ensured that only the people at IIIT Delhi gets access to the web apps. The system defines three types of users namely, Limited user, power user and admin. After authenticating, it is determined that a particular user is of which type. According to the type of the user access is granted to the requested page.

Figure 3.8: User types and their access levels.

Access levels of different users are detailed in Figure 3.8. These applications are described in the next section.

3.5 Applications

As a part of this work, some applications have also been developed which utilize the information given by the system. All these applications have been tied together in one front-end user interface. All these applications have been deployed at IIIT Delhi. These applications provides the users with real-time data. The application are namely, Schedule logging, Time spent, Presence Calendar and Daily metrics, which will be discussed in the subsequent sections.

3.5.1 Schedule Logging

Time is the most valuable asset that any individual has on his hands. It is therefore essential for all individuals to manage their time very effectively. For effective time management one must follow a strict schedule which allows for adequate time for work as well as play.

This application aims at helping people at IIIT Delhi discern their daily schedule. It is a ubiquitous solution which presents the location logs of an individual using his mobile device. This application takes input the MAC address of the mobile device which one carries with oneself all the time and it outputs the visited places, at what time and how much time was spent there. This application is useful for students as it can help them with managing their college time. It helps them in figuring out their study-to-play ratio i.e. out of the eight hours of college time, how much time is spent in canteen, roaming around or playing versus how much time is spent in classes, labs or self-study. For staff or faculty it is useful in discerning how much time they spend in their offices, taking classes, working or at the canteen for lunch or coffee. Figure 3.9 shows the tabular schedule or a timeline of an individual.

Since	Location & Duration	
WED JUN 29 21:15:31 IST 2016	Disconnected	4 hr 29 sec
WED JUN 29 21:09:31 IST 2016	Boys Hostel Floor 0	6 min
WED JUN 29 19:04:31 IST 2016	Boys Hostel Floor 3	2 hr 5 min
WED JUN 29 19:04:24 IST 2016	Boys Hostel Floor 2	7 sec
WED JUN 29 16:41:28 IST 2016	Boys Hostel Floor 3	2 hr 22 min 47 sec
WED JUN 29 16:35:38 IST 2016	Disconnected	5 min 50 sec
WED JUN 29 08:32:24 IST 2016	Boys Hostel Floor 3	8 hr 3 min 14 sec

Figure 3.9: Schedule logging tabular view.

This application gives access to recent schedule history. This application does not store any information related to one's location, the schedule history is obtained from the traps database at the time of request.

The application also provides a way to access one's schedule for a particular day or for some specific duration. One can enter from and until dates to receive the schedule for that particular duration only. This is useful if someone wants to see his last Monday's schedule.

What if someone has more than one mobile device with him, which he interchanges from time to time? This application allows one to input up to two devices and see one's schedule by intermingling the schedule of the two devices. One can also combine the results of his mobile phone and laptop together. Figure 3.10 shows the combined timeline of two devices.

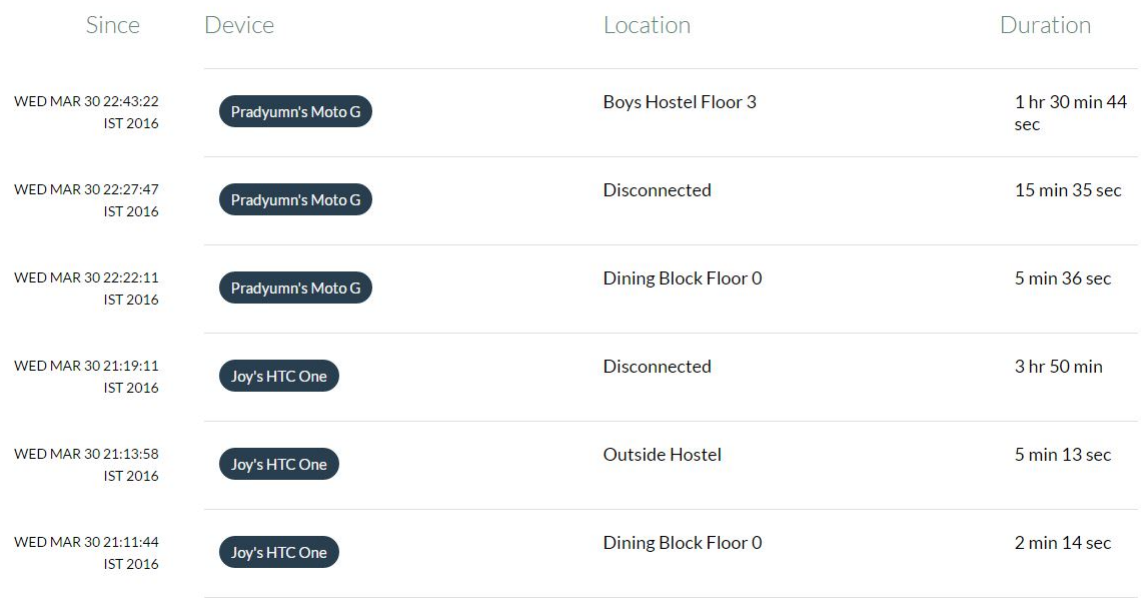

Figure 3.10: Schedule logging for multiple devices.

Schedule Charts

The application offers the users to view their daily schedule using a stacked column chart instead of tabular view. This chart helps in a quick overview of one's timeline. This chart colour codes the different locations and present it on a time axis. One can also remove or select a particular location and view only that location's schedule. This chart allows for zooming on time axis. These charts have been developed using Highcharts[4].

[4]JavaScript API for designing interactive charts for web pages by Highsoft

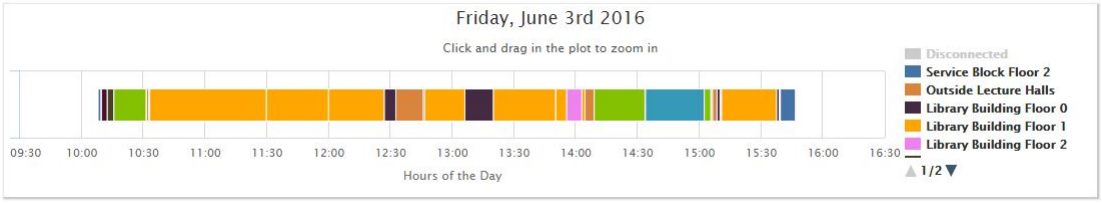

Figure 3.11: Schedule logging chart view.

3.5.2 Time Spent

Managing ones time also requires to study the locations where one has spent more time. This application assist the user in figuring out how much time one has spent at different locations between a defined time period. It summarizes the time spent data and draws a location versus time spent bar chart. This application is helpful when an individual wants t know how many hours he has spent in his office on some day. It can also let one know how many hours one has spent at a particular location in one week or month. The drawn chart has locations on x-axis and minutes spent at y-axis. A base-10 log scale is used for the y-axis or minutes spent so that different locations with very high time spent and locations with very low time spent can be seen together in one bar chart. The chart has been developed using Google Charts[5]. Figure 3.12 shows the visualized graph for an individual.

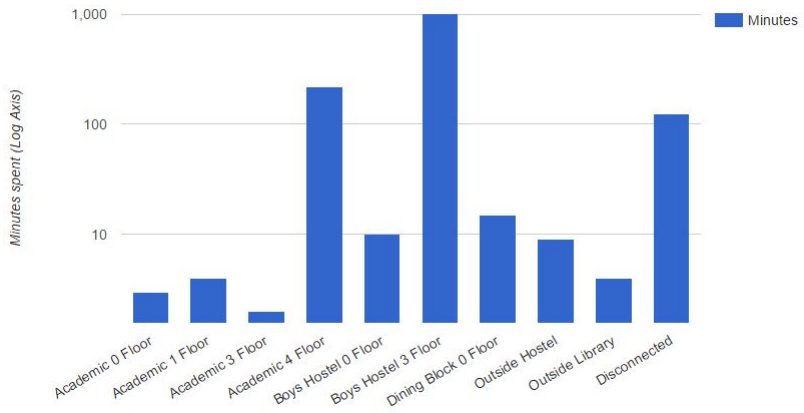

Figure 3.12: Time spent by a user at different locations across campus.

3.5.3 Presence Calendar and Daily Metrics

Presence calendar is the application which marks date on the calendar on which they were present in academic area[6]. This application helps in marking out the present and absent days for students. They can figure out of how many working days they were

[5]JavaScript API for designing interactive charts for web pages by Google
[6]Academic Building and Library Building

present in college. Parameters are fixed for this calendar are that one should go to the academic area between 10 PM to 10 PM on any day. The fixed parameter helps in bringing consistency among all users. Figure 3.13 show such a calendar.

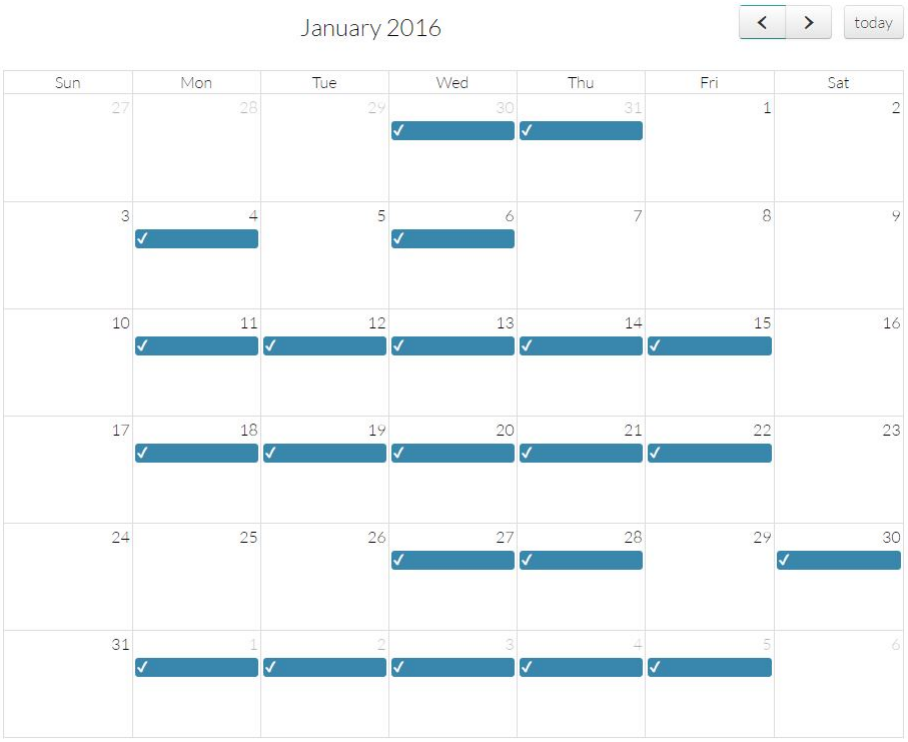

Figure 3.13: Presence calendar of a user.

Custom Presence Calendar

Presence calendar is accessible to all user types including limited user, but Custom presence calendar is only accessible to admins and power users. Custom presence calendar allows for flexible parameters. One can specify the particular building where the presence should be marked. Working hours can also be customized in which one can specify the time period only in which the presence should be marked. Moreover, minimum number of hours spent at that location can also be specified, the time spent at the location is calculated as the total time spent at that location starting in between the specified working hours. The calendar marks the dates on which the criteria is successful. In addition to that, it also specifies the total time spent.

Daily Metrics

It provides the user the timestamp at which he first entered the academic area that day and the timestamp at which the user exited the academic area the day before.

3.5.4 Privacy Concerns

There are certain measures which have been taken for the security and privacy of the users data. The measures are as below:

- The private information in the traps stored in the database are hashed using SHA-256. For instance, the mac and IP address of the device are hashed.
- Google sign-in services are used for authenticating the users. Only the users with valid IIIT Delhi Gmail account are given access to the system.
- There are 3 types of users defined as explained in the section 3.4.2. By default, a user is given the access level of a limited user.
- Authorization schemes enable only the users whose email ID has been added as an admin or a power user will be able to access most of the features.
- Users can store their MAC addresses in their account for quick access. This MAC address is stored in database using the technique Encrypt-then-Hash (EtH) [36]. Encryption is done using AES 256.
- Other than the above, there is no storage of personal data which can lead to privacy breach.

These measures makes sure that even if someone gets a read access to the database, he cannot breach the privacy of the user by interrelating the location logs with the identity of the user. This work does not require the mapping of MAC address to the identity of the individual and assumes it to be private.

Chapter 4

Space Utilization

In addition to the above described applications, this work explores the space utilization at IIIT Delhi. This is incorporated within the system and leverages the trap database. For space utilization, a separate database has been created which stores the data in a usable format. It is achieved by using anonymous location logs of all the devices which are active in a region. It utilizes the system to discover number of people at a particular place for a duration of one hour. In addition to the count of people it also calculates the amount of time spent at that location. These parameters help in figuring out that if the place is optimally used or not. This can also be used for figuring out the involvement of people at a particular event.

For the purpose of analysis of space utilization, two applications have been developed namely, crowd analysis and footfall. The next subsection describes these applications.

4.1 Crowd Analysis

It is the application which converts the anonymous location logs to actual space usage metric. A separate database has been created for storage of this data. This database, referred to as Space Utilization database, is updated every midnight with new location logs of the previous day. Location logs of all the devices present in IIIT Delhi are anonymized and then collated together to give space usage of all the places in the campus. The data is categorized for each place in the campus. The data for each place is further classified for every hour of each day, giving the level of precision for space usage data as each hour.

Man-minute is the metric used for space usage. Although man-minute is a unit for work done, in this work it is used for space usage. This is because work done is analogous to space usage, as here work done is the measure of a person's work for one hour i.e. in other words it is a measure of usage of a person's work per minute, similarly when person occupies a place for a minute then that place is used for 1 man-minute. For instance, if 1 person occupies a place for 60 minutes or 60 persons occupy a place for 1 minute each, then that place is used for 60 man-minutes. Figure 4.1 explains the equality of two cases.

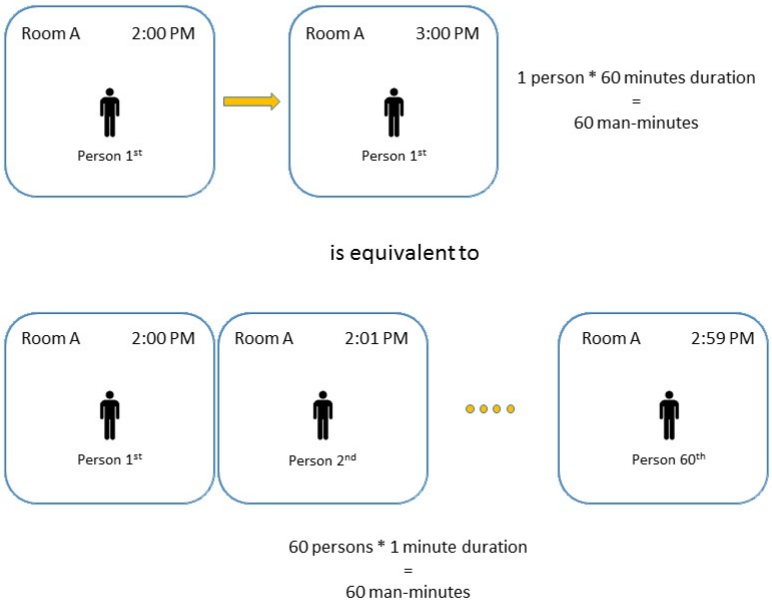

Figure 4.1: Equality of two cases.

Classification of the occupants have also been done. Three classes of occupants have been defined namely Students, Faculty/Staff, and Guests. Man-minutes for every place for all hours of each day for each class of occupants is calculated and stored in the space utilization database. The data is presented to users using an interactive stacked column chart in which man-minutes is on y-axis, months are on the x-axis and stacks represent a day in a month. A user can select a month then the month's days are represented on x-axis and stacks represents every hour of the day. The values on the stack represent the space usage in man-minutes for a unit time. Figure and figure shows the chart. These charts have been developed using highcharts.

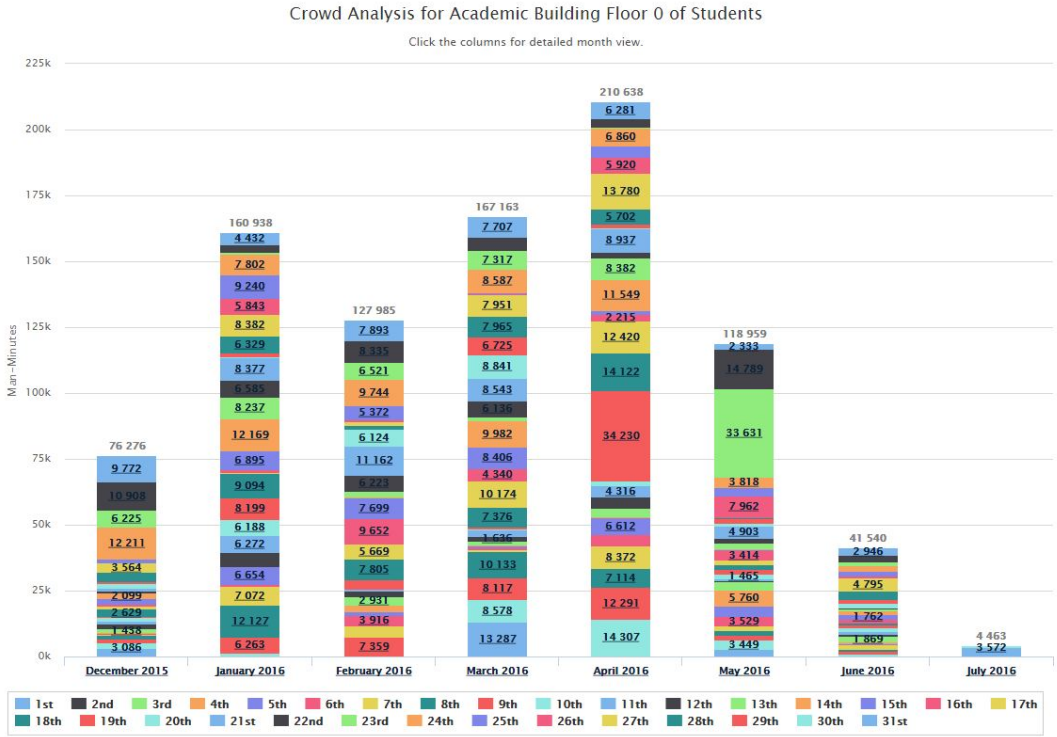

Figure 4.2: Month versus Man-Minutes.

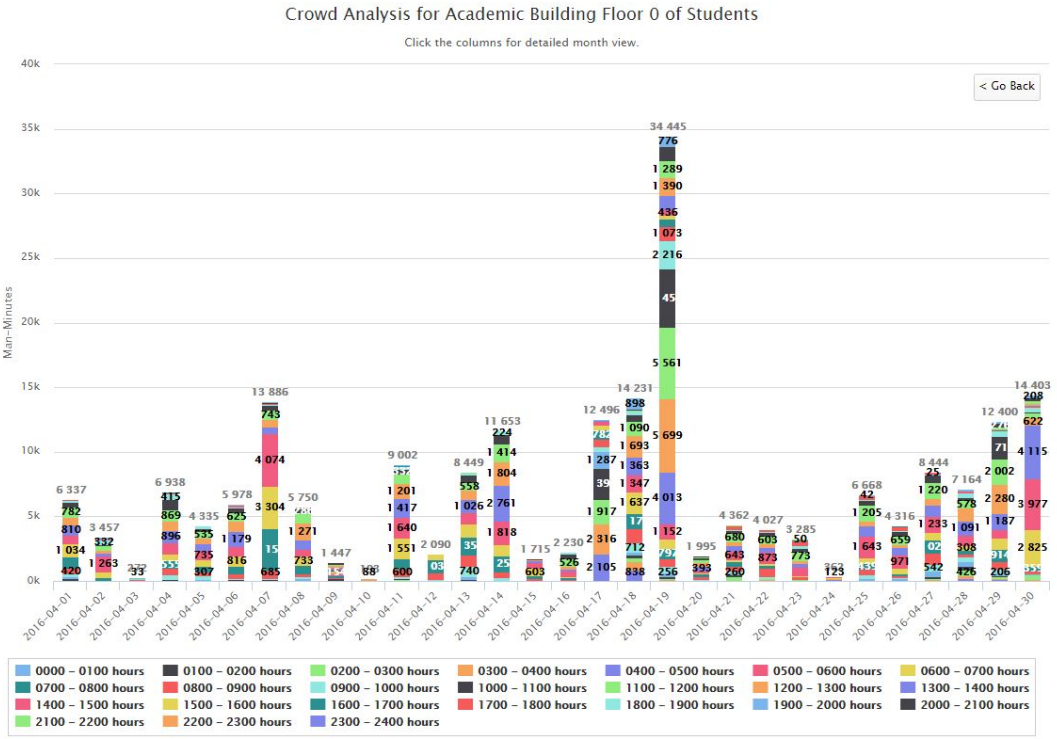

Figure 4.3: Day versus Man-Minutes.

In figure 4.2 and 4.3, it can be observed that on 19th April, 2016 there was a sudden increase of space usage on academic building, ground floor. This was due to the event *Building Better Interfaces, 2016.* Similar sharp increases in data can also be seen, which represents other events. This application can also be used to evaluate the involvement of people at some event.

4.2 Footfall

In the previous application, the combination of number of persons and their time spend is taken into account for calculating space usage while individual contribution of number of people is not taken into account. This application counts the number of people who visited the place irrespective of the time spent by them at that location. This type of analysis help in figuring out the crowd at some place.

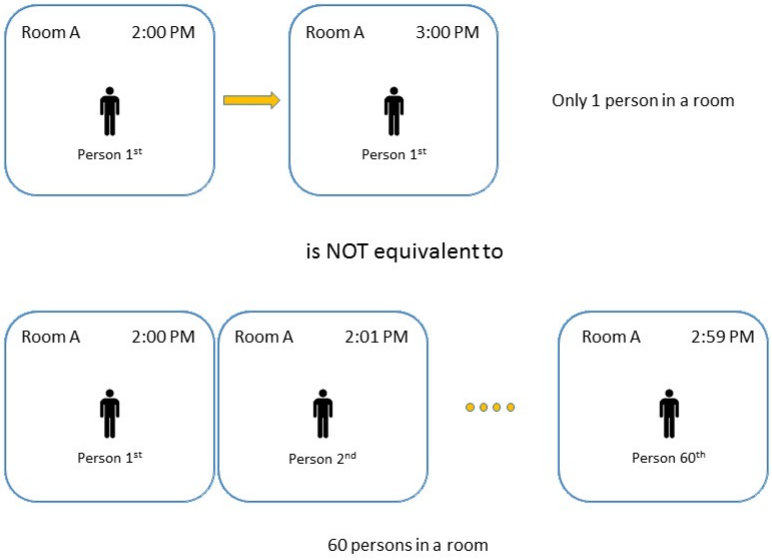

Figure 4.4: Inequality of two cases.

Figure 4.4: explains how this application is different from the previous application. In Crowd Analysis, if a place is used as a pathway for another location then also its usage is shown high but using this analysis only the place where actually the crowd is present is shown. Figure 4.5 shows the footfall charts which are developed using Google Charts.

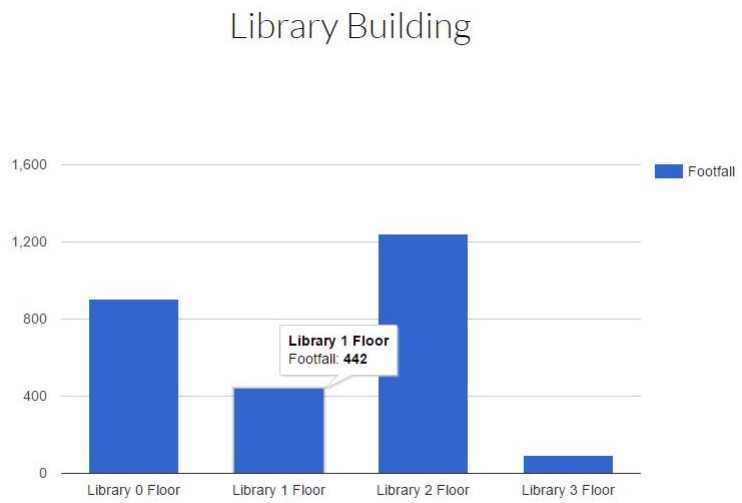

Figure 4.5: Footfall data on some day.

Together these two applications helps in analysing the space utilization of the places in the campus.

Chapter 5

Future Work and Conclusion

As a part of future work, the system can be made more privacy concerned by giving rights to the actual user of the device to authorize use of MAC address - A full-fledged authorization system where a user can give or revoke access any time of the MAC address of his device from any user. Also the applications like Footfall can be improved for faster results by creating a separate database for storing historical data just like crowd analysis application. More insights can be drawn from the data and presented using interactive graphs and charts. Further work can be done to improve the precision of indoor localization to rooms and classes instead of floors and buildings. There are numerous applications which can be built over this system for different perspective of different types of people at IIIT Delhi using the ubiquitous and context-aware nature of the system.

For professors, applications can be developed to have consensus of time of meeting with their students. Further some personal applications like automated mailing system, which automatically construct an email from pre-existing templates and send it to the class representative if he has not reached the class' premises by the time of starting of the class, or mail his members of family whenever he leaves college for home, or acknowledge them when he has safely reached the college in the morning. Many more applications to discern how much one-on-one time has he given to each of his student.

For students, applications can be developed for designing density graphs of the places they visit and spend their time. Similar to the professors, automated mailing system for students can also be developed. Applications for finding their friends in the campus and interesting events happening over at some place.

For network administrators, applications can be developed which point out the locations which are less crowded and switch off some of the access points for saving power, or if people increase beyond a certain threshold, then some access point in vicinity can be turned on to meets the requirements of the crowd.

For administrators and managers, applications for event organizing and deciding venues for the events so that the venues at the time of event is not crowded. Further applications can be developed for context aware HVAC system, which can turn or off according to the number of people present at the place.

For guests, applications can be developed to analyse visitor behaviour so that better services or amenities can be provided. Applications like context aware campus walk-through for visitors, which can help them identify places and roam around the campus.

Using the existing infrastructure of wireless LAN, we were able to build a ubiquitous system for indoor localization. The system is designed to be robust and real-time, and gives access to a secure, easily scalable, elastic and schema-free MongoDB for data storage. Spring web framework allows for building a decoupled system with dependency injection to achieve an abstract design enabling development of applications easy and independent of complexity of the core system. With loosely coupled web applications it ensures the maintainability of the system remains high. Using this system we were able to develop preliminary automated space utilization system for analysing space usage without involving any tedious processes of counting people and taking surveys. It allows the managers to take steps to increase space utilization by maintaining a balance minimising costs and meeting pedagogical and research needs of the staff, and the learning needs of students.

Bibliography

[1] Scott Pace, etal.The Global Positioning System: Assessing National Policies.

[2] b. W. Parkinson and J.J. Spilker - Chapter 1, Global Positioning System: Theaory and Application, vol II, AIAA Publications, 1996.

[3] J. Hightower, Gaetano Borriello. A Survey and Taxonomy of Location Systems for Ubiquitous Computing.

[4] H. Liu, H. Darabi, P. Banerjee, and J. Liu. Survey of wireless indoor positioning techniques and systems, *Trans. Sys. Man Cyber Part C* , vol. 37, pp. 1067-1080, Nov. 2007.

[5] V. Otsason, A. Varshavsky, A. LaMarca, and E. de Lara. Accurate GSM indoor localization. *UbiComp 2005, Lecture Notes Computer Science, Springer-Varlag,* vol. 3660, pp. 141158, 2005.

[6] P. Bahl and V. N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In *Proc. IEEE INFOCOM 2000, Mar.,* vol. 2, pp. 775784.

[7] A. M. Ladd, K. E. Bekris, G. Marceau, A. Rudys, L. E. Kavraki, and D. S. Wallach. Using wireless ethernet for localization. In *Proc. 2002 IEEE/RJS Int. Conf. Intell. Robots Syst., 2002,* vol. 1, pp. 402 408.

[8] A. M. Ladd, K. E. Bekris, A. Rudys, L. E. Kavraki, and D. S.Wallach. On the feasibility of using wireless ethernet for indoor localization. In *IEEE Trans. Robot. Autom.,* vol. 20, no. 3, pp. 555559, Jun. 2004.

[9] J. Barnes, C. Rizos, J. Wang, D. Small, G. Voigt, and N. Gambale. Locata: The positioning technology of the future? presented at *6th Int. Symp. Satellite Navig. Technol. Incl. Mobile Positioning Location Services, Melbourne, Australia [Online].* pp. 4962.

[10] J. Hightower, R. Want, and G. Borriello. SpotON: An indoor 3D location sensing technology based on RF signal strength. In *Univ. Washington, Seattle, Tech. Rep. UW CSE 200002-02, Feb. 2000.*

[11] Space Utilization URL: `http://bmet.wikia.com/wiki/Space_Utilization`

[12] Andrew H. Buchanan, Brian g. Honey. Energy and carbon dioxide implications of building construction.

[13] Zahra S. Moussavi Nadoushani, Ali Akbarnezhad. Effects of structural system on the life cycle carbon footprint of buildings.

[14] M. Weiser. The computer for the 21st century. In *SIGMOBILE Mob. Comput. Commun. Rev.* vol. 3, pp. 3-11, July 1999.

[15] Chen, Y.C., Chan, Y.J. and She, C.W. (2005). Enabling location based services in wireless LAN hotspots. In *Int. J. Network Mgmt.*

[16] Organizational Space URL: `https://en.wikipedia.org/wiki/Organizational_space`

[17] Spatial Science. URL: `https://en.wikipedia.org/wiki/Spatial_science`

[18] K. Gubi. Roughmaps: Indoor positioning using existing infrastructure and symbolic maps, 2010.

[19] A. N. Bharathan Balaji, Jian Xu. Sentinel: Occupancy based HVAC actuation using existing wi-fi infrastructure within commercial buildings. In *SenSys, Conference on Embedded Networked Sensor Systems , 2013.*

[20] RFC 3411 - An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.

[21] RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP).

[22] Abstract Syntax Notation One International Telecommunication Union, Telecommunication Standardization URL: `http://www.itu.int/en/ITU-T/asn1/Pages/introduction.aspx`

[23] SNMP Traps URL: `http://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7244-snmp-trap.html`

[24] M. F. Luca Schenato, Bruno Sinopoli. Foundations of control and estimation over lossy networks. In *Special Issue on Networked Control Systems,* vol. 95, Issue 1, 2007.

[25] IEEE Standards Association, IEEE 802.11 Wireless LANs, URL: `http://standards.ieee.org/about/get/802/802.11.html`

[26] Wireless Distribution System Linked Router Network. URL: `http://www.dd-wrt.com/wiki/index.php?title=WDS_Linked_router_network`

[27] Joseph D. Camp, Edward W. Knightly. The IEEE 802.11s Extended Service Set Mesh Networking Standard. In *IEEE Communications Magazine,* vol. 46, issue 8, pp 120 126, 2008.

[28] Columbia University. URL : `http://www1.cs.columbia.edu/~andreaf/documents/Forte0410_Reducing.pdf`

[29] RFC 1157. URL: —url https://tools.ietf.org/html/rfc1157

[30] Hexagonal Architecture. URL: `http://alistair.cockburn.us/Hexagonal+architecture`

[31] Cisco Object IDs. URL: http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

[32] Cisco Prime Infrastructure Configuration Guide, Release 1.2, URL: http://www.cisco.com/c/en/us/td/docs/wireless/prime_infrastructure/1-2/configuration/guide/pi_12_cg/hard.html

[33] NetDisco MIBs Data Stats. URL: http://sourceforge.net/p/netdisco/mibs/ci/ccef5c1747eda011cae2714b6716cb400130af9f/tree/cisco/CISCO-LWAPP-DOT11-CLIENT-MIB.my

[34] NetDisco MIBs Security Traps. URL: http://sourceforge.net/p/netdisco/mibs/ci/ecaaabccb49ab8d43db00a8cfd77482e963fc679/tree/cisco/CISCO-LWAPP-SI-MIB.my

[35] Martin, Robert C. (2003). Agile Software Development, Principles, Patterns, and Practices. Prentice Hall. p. 127-131.

[36] OEM. URL: http://cseweb.ucsd.edu/~mihir/papers/oem.pdf

[37] Net-SNMP URL: http://www.net-snmp.org/

[38] Wireless Local Area Network URL: http://www.cs.uccs.edu/~gsc/pub/master/pjfong/

[39] Components of SNMP URL: https://www.manageengine.com/network-monitoring/what-is-snmp.html

[40] WLAN Distribution URL: http://lyle.smu.edu/emis/news/?p=36

Appendix A

Data Storage Schemas

A.1 Trap Data Storage Schema

Attribute	Description
ID	unique identifier for each trap
ObjectID	type of SNMP object
timestamp	time and date of receiving the trap
daySerialNo	trap serial number in a day
bsnStationAPMacAddr	AP MAC address
bsnUserIpAddress	connected device's IP address
bsnStationMacAddress	connected device's MAC address
bsnAPName	AP name or symbolic location code
cldcClientMacAddress	connected device's MAC Address
cldcApMacAddress	AP MAC address
cLApName	AP name or symbolic location code
clrRrmNeighborApCount	the number of neighbours of an AP
clrRrmNeighborApMacAddress	list of MAC addresses of neighbour APs
clrRrmNeighborApRssi	list of MAC addresses of neighbour AP's RSSI values
cldcClientSSID	connected device's SSID
cldcClientSessionID	connected device's session ID
cLApSysMacAddress	MAC Address of the AP
cLSiIdrDeviceId	interruption device ID
cLSiIdrDeviceType	interruption device type
cLSiIdrAffectedChannels	Channels in which there is interruption
cldcClientIPAddress	connected device's IP address

Table A.1: Trap data storage schema.

A.2 User Data Storage Schema

Attribute	Description
emailID	IIIT Delhi's email ID of the user
namedHashEncryptMacList	list of named hashed encrypted MAC A.3

Table A.2: User database schema.

Attribute	Description
name	name of the saved device
img	image code for the saved device
hmac	hashed and encrypted MAC

Table A.3: Named Hashed Encrypted MAC object