Communication Protocol and Queuing Theory-based Modelling for the Internet of Things

Sandesh Mahamure[1], Poonam N. Railkar[2] and Parikshit N. Mahalle[2]

[1]*Department of computer engineering, Savitribai Phule Pune University, Pune, India 411041*
[2]*Smt. Kashibai Navale College of Engineering, Pune, India*
E-mail: {s.mahamure; poonamrailkar; aalborg.pnm}@gmail.com

Received 19 January 2016;
Accepted 28 February 2016

Abstract

Internet of things (IoT) is communication network in which the devices are connected to each other via internet. World is moving towards the atomization of various domains of engineering. The growing applications of IoT imposes challenge on the user to manage all such application. This paper proposes Internet mail Access protocol (IMAP) for IoT enabled email system. It helps to reduce the application Management overhead from the user side. It provides common platform for managing applications to the user. At the same time this protocol should not compromise with security.

The advantage of IMAP is that user can access mail system ubiquitously. This paper proposes architecture in which middleware is introduced for the interoperability platform. Also it proposes mathematical model with the help of M/M/N queuing model. This paper supports proposed mathematical model with the help of proof of concept.

Keywords: IMAP, Internet of Things.

Journal of ICT, Vol. 3, 157–176.
doi: 10.13052/jicts2245-800X.323

1 Introduction

Internet of things is a communication network for things. The things can be any sensors, actuators or any devices. The concept of IoT first introduce in 1999. The main motivation of IoT is atomization of all fields of engineering. IoT is collection of various technologies under single umbrella. In this fast and running world, time and money are two major factors can be saved by these connected devices. The data generated from these devices can be used for decision making. Now software industries like Microsoft, Google and Facebook are interested to invest their knowledge and resource in the Domain of IoT. Many of the European countries view IoT as an opportunity of growth and development and they have started the smart city project. European commission started various project in the domain of IoT. Now Indian government has also launched the smart city project and ready to invest resources for smart cities.

In future there are billions and trillions things are going to be connected, in this case it is necessary to uniquely identify each and every device so the addressing problems can be removed by the IPv6 addressing strategy. IPv6 addressing uses 128-bit internet addressing scheme used to replace IPv4 addressing strategy which were officially declared outdated. IPv6 gives ease in the identification of devices.

IPv6 supports auto configuration of network and easy to manage and configured automatically once they are in network. There are various challenges in the IoT related to privacy and security, data ownership etc. There is no standard generic architecture for IoT for the reference. The current devices unable to scale towards IoT services, so large number of resource entries may lead to delay. Cloud computing also plays an important role in IoT. Cloud computing has its services providing model which are software as a service (SaaS), Platform as a service(PaaS) and Infrastructure as a service (IaaS). For example, PaaS provide platform to access IoT data and on which the applications can be developed. Wireless sensor network gives foundation to connect the different devices with different capability. There are various application domains of IoT for example Agriculture, Supply chains, Governments, Retail, Transportation, Energy Management and other domains also. The Figure 1 shows mapping the OSI layered protocol suite to IoT protocols. XMPP, MQTT, CoAP are present in application layer which provide interface to user. Other protocols provide functionality according to the layer. In this Paper after the introduction Section 2 describes motivation of proposed work. Section 3 provides related study. Section 4 describes about gap analysis. Section 5 provides details about

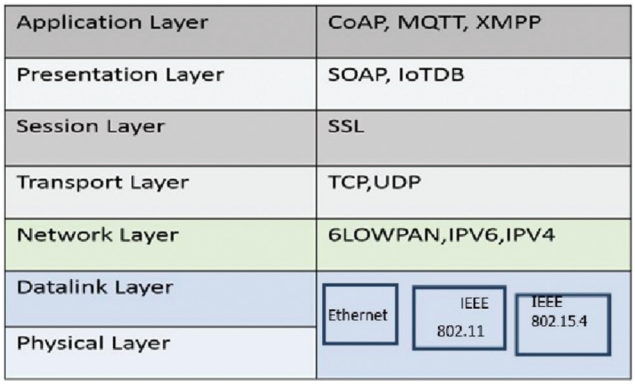


Figure 1 IoT protocol suite.

proposed architecture. Section 6 discuss about proposed mathematical model based on queuing theory. Section 7 proposes suitable concept of proof and finally Section 8 describes conclusion of this paper.

2 Motivation

Consider a person who developed his home completely automated and he manages his home via application at the same time he has variety application related to the smart vehicle, application which finds the empty parking slot in the parking, health related applications, automated office and etc. In this scenario user of the system has an overhead of managing all the applications. User needs to keep records of certain notification related business. All these applications use user's smart phone precious main memory, so that user needs the common platform through which user is able to manage all the applications. Email can be used as a common platform through which all the applications user can manage. Email is reliable way of communication. It can handle any type of data i.e. text or Multimedia. User can classify mails according to his requirements. Email has its own security mechanism through which users can maintain their privacy and other security related issues.

3 Literature Survey

In European countries they had started a collaborative program called FP7 (7th Framework Program for Research and Technology Development) to fulfill need of these countries as well as improving living standard. This program

mainly emphasis on the projects which are related to Internet of Things. They invest their funds in novel projects.

3.1 E-WALL

It provides services to those adults those who wants to live independently and suffering from physical disability due to their old age. There are primary and secondary users. Primary users further divided into three categories, 1) Elderly with age related Impairments (ARI) 2) Chronic obstructive pulmonary disease patient (COPD). 3) Elderly suffering from mild dementia. Secondary users group consists of general practitioner, hospital nurse, visiting nurse, friends, relatives and caregivers or it can be categories into caregivers and caretakers. The main objective of E-wall project an independent living of adults and provide communication framework for primary and secondary users. When we consider healthcare support phone and video call is used to do communication between primary and secondary users [3].

3.2 CuteLoop

Cuteloop gives new way of engagement of consumer and producer in business network. Food chain management is one of major application domain of this project. The main objective of Cuteloop is not to change existing scenario but to add more features by using the networked devices. The elements in this scenario are 1) Access Network which represents the entry point for the user in Cuteloop solution and provides access to CuteLoop services and functionality. 2) Services and Agents: – These represents an ICT based functionalities and features. The services are categorized into mainly three types of services are as Basic, Security and Interaction. The basic services enabling the architecture components of the operation. Security services provided to perform secure operation under Information and Communication technologies (ICT) support. It provides basic services like authentication and authorization and finally event driven agents gives asynchronous interaction between actors. The tracking and tracing RFID and Global Navigation Satellite System are technologies used in this project. Cuteloop provide framework for interaction of various heterogeneous ICT applications. The major focus is on the transaction between peer by using public network. These actors may exchange data and actor related data. The human operator centric devices mentioned in this project can use in this project are personal computers; notebooks tablet pc, PDA, mobile phones and smart phones. In smart phone we use SMS, MMS services for communication [4].

3.3 ASPIRE

This project changes current RFID deployment process by introducing middleware which is innovative, programmable, royalty free, privacy friendly and light weight. ASPIRE will reduce considerable cost in small medium scale enterprises for RFID technology by providing this middleware. The ASPIRE middleware works on open source software component which is researched by various OSS communities and developed by consortium. The Traditional RFID which is having mobile tags and these RFID respond to the request by sending the relevant data. The concept of fixed reader is outdated now the tags are fixed and readers are mobile. So we use m-RFID i.e. Mobile RFID. The M-RFID has advantage over traditional RFID is that it has no wires connected to fixed readers and several mobile readers can be served. There are various application domains like Information retrieval, data transmission, automated messaging, etc. in which we can integrate RFID into mobile networks. The one of the major issue in this project is RFID-IPv6 mapping. There are various middlewares but these middleware does not complete all customer expectations [5].

3.4 GRIFS

GRIFS is one of the project fp7 program collaboration with GS1, ETSI and CEN to improve RFID standardization process. The initial task of this project was to produce report on current RFID standards and standardization bodies, the scope of work, opportunities and gap analysis. GRIFS identify potential standard development areas where multiple standard development organization works in participation with each other so that they can reduce overlapping work and avoid unnecessary work. They design a network model in which they classified this model into two groups firstly one is RFID data capture which is concern with technology related aspect and secondly is RFID data process which is strongly concern with data flow. The Process of RFID standardization is started since 1997.ISO IEC, ETSI and ITU-T are the standard bodies which are working at global level. ISO registration authority decides standards about unique item identifiers data dictionary and message standards. There are various application domains where standardization needs to be done in internet of things [6].

3.5 IoT@Work

In automation technology we can generate event triggered messages based on protocol such as SMTP, IMAP and POP3. IoT@work adopt iterative model

for developing architecture of this project. In this project they analyzed three real time scenario cluster i.e. agile manufacturing, large scale manufacturing and remote maintenance. This project overcomes reconfiguration cost. IoT provide plug and work capability to devices in which devices are configured automatically as well as network can be configured automatically. IoT@work focuses on three security aspects. 1) Secure service access 2) Secure plug and work 3) Secure communication [7].

3.6 Ebbits

The main objective of this project is to develop architecture process and technologies which helps business to integrate IoT into enterprise and provide support for end to end business application. The application of this project is automotive manufacturing, agriculture and business domain. The device sensor tags generate data and ebbits act as Communication Bridge between backend enterprise application, people and real world. It has service oriented architecture. Ebbits helps in automation of business workflow from start to end. Now for internet the vision is internet of things and services (IoTS). The ebbits is enabling business based internet of things and services. This project develops interoperability platform for IoTS. The application domains for IoTS are healthcare machine to machine communication and energy efficiency. When there is communication between machines to machine, the telemetry language is used. The machine to machine communication can be used in the traffic control system. Ebbits can be used in domain of energy in two roles first one is production and second is distribution of energy and this is what we called Smart grid. For this there are two approaches first one is contiki and second one is TinyOS. The operating system consists of IP stack present at natively and enabled. The various types of security aspects considered in this project [8].

3.7 i-SURF

Today's competitive and demanding digital world requires to adopt changes made by small medium Enterprises (SME). In business trading partners have different business strategy and they collect data from different sources. If this information is not shared, then it can affect effective decision making and it will lead to loss in business. To solve this issue, we require a distributed intelligent environment for multiple partners in order to fulfil customer demand. i-SURF is an interoperability service utility for collaborative supply chain planning across multiple domains supported by RFID devices. It provides

knowledge oriented platform to share information among the partners for multiple domains. This is done in secure and controlled way. The prerequisite for this platform is infrastructure for information exchange and have a proper definition of business process. Many organizations address the standardization of communication in sharing of information in supply chain process. In response to this problem i-SURF provide interoperability service utility for planning business processes. Operating system consists of IP stack present at natively and enabled. The various types of security aspects considered in this project [9].

3.8 AVANTSSAR

Now IT system and application shifted one generation to next generation due to this change there are lot of issues related to trust and security. These issues are very dangerous due to interference between components, services and shared communication. The AVANTSSAR project is designed to develop such a technology which supports the formal specification and automatic validation of trust and security in Service Oriented Architecture (SoA). The AVANTSSAR project focuses on all aspect of security like Authorization, Authentication and Access control etc. Due to this AVANTSSAR is widely accepted. The project consists of some component 1. AS LAN: It is trust and security aspect of services that specifying modelling languages. 2. Develop novel automated technique 3. AVANTSSAR validation platform for validation of trust and security aspect of SoA. 4. Library of secure service oriented architecture and services [10].

3.9 TRACER

This is a FP6 funded project which has scientific and technological objectives. The basis for this project is mapping of identity of product to identity specific tracking and tracing. The main achievement of this project is open source tracking and tracing solution platform.

ID@URI is responsible for uniqueness of identifiers. The key application domain of this project is logistics and asset management. The advantage of this project is location and Status of asset provide to the user. This project helps in automation of inventory and helps to identify that what is present in the store. The user continuously tracks his asset. In TRASER the data is associated with individual assets. These data related to item is stored on network server along with identifier of product [11].

3.10 Thunderbird

It is open source email client developed by Mozilla foundation. Now Mozilla focuses on the development of thunderbird. The features of Mozilla thunderbird are message management, junk filtering, support various extensions and themes. It supports various standards. It is also news client and chat client. We can receive feeds from various news and social networking sites [12].

[13] The authors of this paper et. al. security perspective required for communication in IoT. This paper discusses about steps taken by Internet Engineering Task Force (IETF) in order to build generic security solution set for any IoT system. It discusses how Constraints Application Protocol can be work in collaboration with standard security protocols. This paper also gives brief explanation about the need of standardization in IoT for increasing interoperability as well as smoother way to adopt IoT by the industry for better security solution. The various standardization bodies like IEEE, IETF and W3C are working on different layer for the motive to provide security at each layer in the architecture. The guideline provided by IETF will be beneficial to design efficient protocol.

[14] This paper proposed generic procedure for communication of objects in IoT. It also provides guidelines which will provide strong base to build communication protocol standards for IoT communication Network. In this paper authors addresses two technical problems that are standards and protocols. To get correct result from analysis two factor are very much important that are status of data and timeliness of the data and based on these factors protocol standardization needs to be done. Static data and dynamic data are the two types of data and based on rate at which data is updated the classification of data needs to be done. Values of dynamic data are changes with respect to time domain. The detailed information related to particular UID. Static data consist of unchanged data related to UID over long period. The timeliness of data can be defined in terms of validity period of data. It can be short period, long periods and permanent data. This paper focus on food inspection. This paper also proposes guidelines for designing application layer protocol.

[15] In this paper authors have given description about transreceiver module which is required for wireless communication and successfully deployed in building monitoring system. The authors demonstrated the idea of smart receiver which supports ZigBee, Wi-Fi, and Bluetooth communication protocols. The main motivation behind this project is to build a middleware which allows communication between various communication protocols in IoT which will leads to smart and intelligent system. The future scope of this

transreceiver is to develop with ardiuno development module and provide platform for multiple generic protocols.

[16] In this paper authors proposed architecture for holistic network which consist of embedded system and for communication, protocols are used. This architecture has built on strong foundation of Service Oriented Architecture. The application layer protocol CoAP and standard services exchange information with public as well as private cloud. This cloud is also connected with smart IoT devices. This architecture also makes a provision for controlling the sensor data. There are some Quality of Service (QoS) parameters are needs to be taken under consideration to support various types of smart application. There is scope to improve security when data is sent to public cloud or network.

[17] The authors of this paper proposes secure data transmission protocol. This protocols helps to improve the security for data transmission. The Internet of Military Things (IoMT) is the interconnection of military things in IoT concept. The proposed protocol is designed for the data link layer with the help of trusted authenticated module. These protocols can be embedded in system. M node in the module manages the authentication of sensor which participate in the process of data exchange between sensors. When data is sent from S node to M node the data needs to be encrypted. S node stores the keys in their own resources which are secured. This paper also Proposes implementation method of proposed protocols.

4 Evaluation of the Related Works

In Gap analysis we consider various factors, comparison parameter among some projects of FP7. The notification on email represents the physical layer devices which send the data to the user with the help of email as well as it sends the notification on mobile. In the event triggered massaging if any specific event is occurred then the message is send to user automatically. The server and storage required for user is present in cloud and it provides scalability to server. In the message grouping the message is grouped according to devices. There are two inboxes in which first one is for user and second is for devices. The backward compatibility parameter is based on compatibility with legacy system. The following shows the gap analysis for FP7 project.

The major problem with these projects is that there is no common platform. All the projects work on different platforms or applications. The user needs to manage all the application independent. Majority of application does not

Table 1 Gap analysis

Parameter	Email Notification	Notification on Smartphone	Notification on Social Media	Event Triggered Messaging	Server and Storage on Cloud	Message Grouping	SMS Grouping	Backward Compatibility
E-WALL	NO	YES	NO	NO	–	NO	YES	–
CuteLoop	NO	YES	NO	YES	YES	NO	YES	NO
ASPIRE	NO	NO	NO	–	–	–	–	YES
GRIFS	NO	–	–	–	–	–	–	–
IoT@Work	YES	YES	NO	YES	YES	NO	YES	YES
Ebbits	NO	–	NO	–	–	–	–	YES
i-SURF	NO	–	NO	–	YES	–	–	YES
AVANTSSAR	NO	–	–	–	–	–	–	YES
TRACER	NO	YES	–	–	N0	–	–	–
Thunderbird	YES	–	–	–	–	YES	NO	YES
Proposed System	YES	YES	YES	YES	YES	YES	YES	YES

concern with the email notification. User should be able to manage all his devices through the email because email is common for user and user is also aware of handling email. Some projects have their own application so that they can send notification to smartphone. The use of social media is tremendously increased so there is need to send notification on social media to inform user about event. In event triggered messaging if any uncertain event is occurred then system should generate notification and send it to the user accordingly. The application server should be present over the cloud then the all security aspect of user data should be taken under consideration like data ownership, privacy preservation, authentication and identity management and access control. We can send only limited text data with SMS service. There is no provision of multimedia data. Backward compatibility helps to reduce infrastructure cost.

5 Proposed Architecture

In this section the proposed architecture is Email based IoT communication network. The proposed architecture focus on how IMAP protocol can be used for IoT system. In this scenario the things, sensors, actuator or devices will connect together via internet. The devices can be any home appliances or any real world objects. These devices or sensors will send the data to the data collection node or middleware where the business logic is present. At the middleware data is aggregated as well as filtered. The aggregated data is then use to build context – aware environment for smart system. After preprocessing of sensor data or device data it will convert into user required email format. Middleware is used to provide the interoperability platform as well as support to the legacy systems. In middleware the data collection node and other components shown in Figure 2 can be placed together or in distributed manner. In real time gateway devices will be act as a middleware. In distributed environment by using SMTP protocol, the mail is transferred from one Mail Transfer Agent (MTA) to another. This mechanism is analogous to the client server Architecture. IMAP server will be present on the cloud so that the system can be scalable as per the growth of the users. The devices will be registered under device owner's account so that they can be accessed by only device owner. So this way privacy and security of the proposed system will maintain. If any action taken by the system then notification will be send to social media, email, application which is already installed in smart phone of user. At the same time SMS notification will be send on user's smartphone. The message grouping is required for the user convenience. The IoT message will

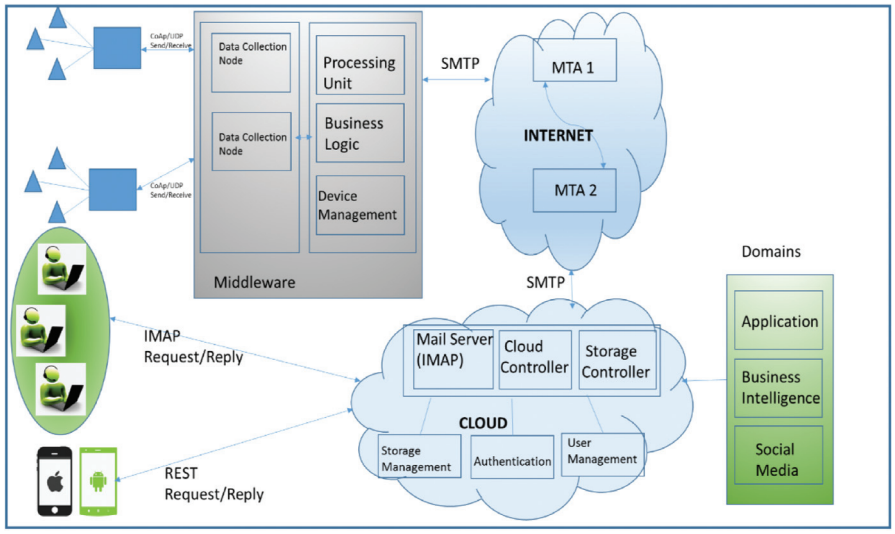


Figure 2 Proposed architecture.

be separated from normal messages that is what we call message grouping. The IMAP server is present over cloud which will provide flexible proposed system. The main two key participants of the cloud that are

a. Cluster controller: – it manages operations within the clusters and
b. Storage controller: – it controls the storage related operations.

Authentication and user management task also handled by these servers. The data generated by sensor devices and other devices can be stored over the cloud and can be used for various application domain like agriculture, business intelligence, etc. The proposed architecture is shown in Figure 2.

6 Proposed Queuing Theory based Mathematical Model

Proposed system can be modeled based on queuing theory. In the proposed system client used email as a communication protocol and this email is processed by the server. To handle the request from number of client system require M identical server. M identical server require mainly for load balancing. The arrival rate of email is distributed randomly in time domain. The service time is also exponentially distributed so we require a M/M/N queuing model to represent our system. A is the arrival rate of an email to the server and L be the packet length and B be the bandwidth of network. Network delay is important

characteristic need to be taken into consideration in the performance analysis of network. The delay varies from network to network. Sometimes congestion in the network may be responsible for the delay. In packet switching network the time required to process a packet by a node is called processing delay. In some network the processing delay needs to be neglect but in the proposed system time is required for the processing of email in the middleware. Another delay needs to be taken into consideration is that queuing delay. The queuing delay can be defined as the time which is spent by the packet in queue until it is processed. The number of Email being served is consider as service time.

$$\text{Service Time (S)} \;=\; \text{M}\frac{L}{B} + \text{Q}_\text{d} + \text{P}_\text{d}$$

Where Q_d is queuing delay and P_d is processing delay. After simplification we get

$$\text{Service Time (S)} \;=\; \frac{L}{B}(M \;+\; A) + \text{Pd} \tag{1}$$

Processing delay is strongly depending on routers capacity not on the packet length Departure rate is also affected by these two delays. Departure rate can be determined by following Equation.

$$\text{Departure Rate (D)} = \frac{1}{\frac{L}{B}(M \;+\; A) + Pd} \tag{2}$$

Utilization of server the time for which server is busy. The utilization of server always $0 < \text{U} < 1$. Utilization (U) of the server can be determined by the following formula.

$$\text{Utilization (U)} = \frac{A\left(\frac{L}{B(M \;+\; A)+Pd}\right)}{M} \tag{3}$$

The waiting time of mail in the system is the fraction of time for which mail is waiting in the queue. Total time is total time spent by the mail in the system and consist of waiting time and service time.

$$\text{Total Time (T)} = \left(\frac{L}{B}(M \;+\; A) + Pd\right)(N+1) + R \tag{4}$$

Where T is total time and N is total No. of messages and R is the residual time. Residual time represents a time that newly arriving devices a non-empty queue has to wait in the queue [1].

At the equilibrium state condition, we need to consider arrival and departure of mails at each state.

By summing up all state probabilities

$$1 = \mathrm{P}_0 \left(\sum_{k=0}^{m-1} \left(\frac{\frac{L}{B}(M\ +\ A) + \mathrm{P_d}}{M} \right) k - \frac{1}{K!} \right.$$

$$\left. + \sum_{k=m}^{\infty} \left(\frac{A\left(\frac{L}{B}(M\ +\ A) + \mathrm{Pd}\right)}{M} \right) k \right) \tag{5}$$

So Equation (5) gives all state probabilities which is equal to 1. To support proposed mathematical model, the proof of concept is also given in next section.

7 Proof of Concept

In the following section the performance of proposed system shown graphically. The performance of proposed system analysed by considering various parameters and proposed mathematical model. In this analysis keep the bandwidth and packet length constant and arrival rate is varying. The processing delay strongly depend on the routers capacity. There is no impact of packet length on the processing delay. Arrival rate of email in the system is exponentially distributed or randomly distributed in time domain. After the arrival of email in the system it waits in the queue for processing so we need to consider the queueing delay of the email.

In proposed mathematical model we consider the constant processing delay so the Figure 3 shows the graphical relationship between utilization and arrival rate. As the arrival rate of email increases the utilization of the system also increases but after threshold it will be constant. While analysing proposed mathematical model three identical servers are taken into consideration. As shown in Figure 3 we consider four values of arrival rate i.e. 5, 10, 15 and 20 messages/sec in order to show behaviour of the system with respect to Utilization of the server. The sharp bent in the curve represents as the arrival rate approaches to the maximal value then utilization of the system also approaches to the maximal value.

The following Figure 4 shows the relationship between Departure rate and utilization. As the departure rate increases utilization of the system decreases. The results are same as the standard M/M/N Queueing model. The departure rate depends on the service rate. Utilization mainly depends on arrival rate and

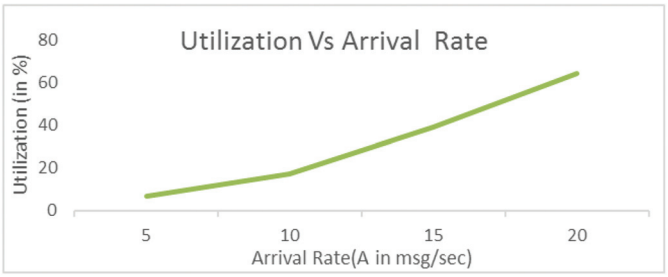


Figure 3 Utilization vs arrival rate.

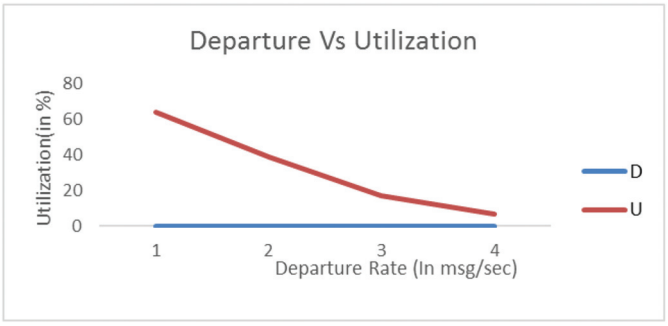


Figure 4 Departure vs utilization.

departure rate of the email in the system. As shown in Figure 4 we consider four values of departure rate i.e. 0.103, 0.125, 0.195 and 0.25 messages/sec in order to show behaviour of the system with respect to Utilization of the server. The sharp bent in the curve represents as the departure rate approaches to the maximal value then utilization of the system approaches to the minimal value. The Figure 4 supports the Equation 3 in the proposed mathematical model.

At the equilibrium condition as the no. of server increases the departure rate is also increases but after certain threshold it will be remains constant. From the graphs we can conclude that the processing delay and queueing delay can affect the performance of the system. The total time the message in the system is dependent on three factors i.e. service time, waiting time and residual delay. Addition of queuing delay and processing delay in the service time increases the total time of message in the system.

The above Figure 5 shows the relationship between Service time and departure rate. As the Service time increases departure rate of the system decreases and vice versa. The nature of graph shows the same behaviour as the standard M/M/N queueing model. As the service time increases the total time

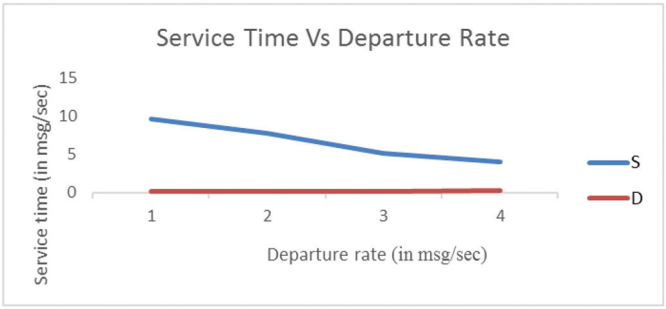
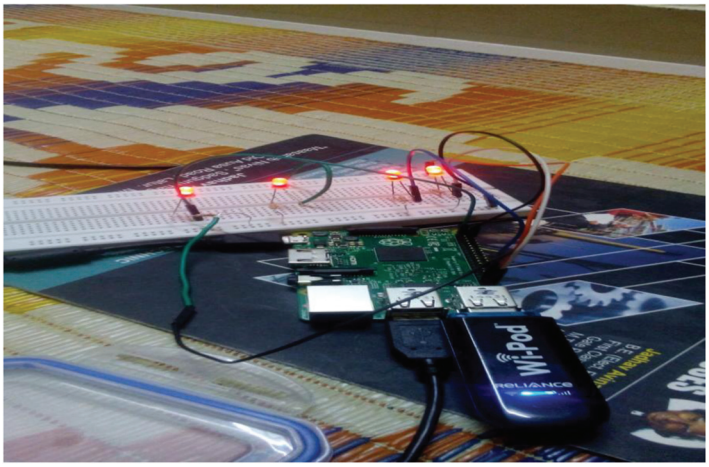


Figure 5 Service time vs departure rate.

for the message in the system also increases. It can affect system performance. The Figure 5 supports the Equation 2 in the proposed mathematical model.

8 Implementation

The following Figure 3 Shows the implementation of the proposed work. The LED is connected to the raspberry- pi micro controller which acts as middleware. At the same time, it is working as data collection node. If we connect sensor nodes to raspberry- pi module the data is aggregated at the Raspberry Module. The aggregated data is preprocessed and filtered at raspberry module with the help of raspberry module, we can access and monitor the devices at the remote place. At the other end IMAP server has been



configured and provision is also made in the server to access the devices via raspberry module. IMAP server deployed over cloud for accessing devices ubiquitously. Cloud also helps to manage load distribution among all the instances of the server. When LED is on and user wants to make it off provision has been made to switched off the LED. Raspberry module will send notification to the user on his smartphone as well as email account. These LED can be replaced by any electronic appliances. The devices can be accessed by only authenticated user who are owner of these devices. This will become a generic communication framework.

9 Conclusions and Future Outlook

Thus this paper has explained the need of IMAP protocol in the IoT communication network and also the role of middleware to provide interoperability platform as well as support to the legacy system. Introduction of IMAP protocol in IoT helps to provide common communication platform for all applications and it reduces the application management overhead and also saves mobiles precious main memory. Deployment of mail service on the cloud offers scalability to the system. We also extended the M/M/N queueing model to our proposed architecture with the delays. To support proposed mathematical model, this paper also gave suitable proof of concept. In proof of concept the graph generated by proposed mathematical Equation shows same nature as the standard M/M/N queueing model. In future we need to design lightweight IMAP protocol for device to device consumption.

References

[1] Nancy, A. P., Railkar, P. N., and Mahalle, P. N. (2014). "A queueing theory based modelling for performance analysis towards future internet," *in IEEE 2014 India Conference (INDICON)*, Pune. doi: 10.1109/INDICON.2014.7030521

[2] Kershenbaum, A. (1993). *Telecommunication Network Design Algorithms*. New Delhi: Tata McGraw Hill.

[3] eWall. Available at: http://ewallproject.eu/

[4] CuteLoop. Available at: www.cuteloop.eu

[5] Aspire. Available at www.fp7-aspire.eu

[6] UniWeb. Available at www.grifs-project.eu

[7] IoT@Work. Available at https://www.**iot**-at-**work**.eu/

[8] Available at www.ebbits-projects.eu
[9] Srdc. Available at www.srdc.com/tr/projects/isurf
[10] AVANTSSAR. Available at http://www.avantssar.eu/
[11] Joomla Traser. Available at http://www.traser-project.eu/
[12] Thunderbird. Available at https://www.mozilla.org/thunderbird/
[13] Keoh, S. L., Kumar, S. S., and Tschofenig, H. (2014). Securing the internet of things: a standardization perspective. *IEEE Internet Things J.*, 1, 265–275. doi: 10.1109/JIOT.2014.2323395
[14] Liu, Z., Xi, B., and Yuan, Y. (2012). "Analysis on IOT communication protocol," in *IEEE International Conference on Information and Automation*, Shenyang, China.
[15] Gunasagaran, R., Kamarudin, L. M., Zakaria, A., Kanagaraj, E., Alimon, M. S. A. M., Shakaff, A. Y. M., et al. (2015). "Internet of things: sensor to sensor communication," in *IEEE 2015 Sensors*, Busan. Doi: 10.1109/ICSENS.2015.7370448
[16] Pereira, P. P., Eliasson, J., Kyusakov, R., Delsing, J., Raayatinezhad, A., and Johansson, M. (2013). "Enabling cloud-connectivity for mobile internet of things applications," in *IEEE Seventh International Symposium on Service-Oriented System Engineering*, Redwood City, 518–526.
[17] Chudzikiewicz, J., Furtak, J., and Zielinski, Z. (2015). "Secure protocol for wireless communication within Internet of Military Things," in *IEEE 2015 2nd World Forum on Internet of Things (WF-IoT)*, Milan, 508–513. doi: 10.1109/WF-IoT.2015.7389106

Biographies

S. Mahamure is Teaching Associate in Department of Computer Engineering at STESs Smt. Kashibai Navale College of Engineering, Pune. He has obtained his B.E. in Information Technology from Shivaji University,

Kolhapur, India. Currently he is pursuing his Masters in Computer Engineering at STESs Smt.Kashibai Navale College of Engineering, Pune. He can be reached at s.mahamure@gmail.com. Research Area: Internet of Things.

P. N. Railkar received her Master in Computer Engineering (Computer Networks) from Pune University Maharashtra, India in the year 2013. From September 2012, she is currently working as an Assistant Professor in Department of Computer Engineering, STES's Smt. Kashibai Navale College of Engineering, Pune, India. She has published 15 plus papers at national and international journals and conferences and authored 1 book. She has guided more than 10 plus under-graduate students and 3 plus postgraduate students for projects. Her research interests are Mobile Computing, Identity Management, Security and Database Management System Applications. She can be reached at: pnrailkar@sinhgad.edu, poonamrailkar@gmail.com

P. N. Mahalle has obtained his B.E. degree in Computer Science and Engineering from Sant Gadge Baba Amravati University, Amravati, India and M.E. degree in Computer Engineering from Savitribai Phule Pune University, Pune, India. He completed his Ph.D. in Computer Science and Engineering specialization in Wireless Communication from Aalborg University, Aalborg, Denmark. He has more than 15 years of teaching and research

experience. He has been a member board of studies in computer engineering, Savitribai Phule Pune University (SPPU), Pune, India. He has been a member – Board of studies in computer engineering, SPPU. He is member – BoS coordination committee in computer engineering, SPPU. He is also serving as member – Technical committee, SPPU. He is IEEE member, ACM member, Life member CSI and Life member ISTE.