International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7, Issue-6, March 2019

Software Engineering Oriented Approach for Iot Applications: Need of the Day

Darshan Pradeep Pandit, Sudhir Ranjan Pattanaik

Abstract*: *The IoT devices are growing faster in which televisions, vehicles, camera, home sensors, computers, peoples, animals and other things get connected to internet very easily and communicate with each other. These devices should be properly managed and controlled with the general set of rules which helps their stakeholders in terms of issues like security, confidentiality, interoperability, reusability, flexibility. The IoT devices require a novel software engineering approach for modelling and design which can deal with the above issues. This research paper provides a precise view and the need of novel software engineering approach for IoT devices.

Index Terms*: *IoT, Software Engineering, Heterogeneity, Interoperability.

I. INTRODUCTION

Today's world is connected with Internet of Things (IoT) by involving sensors, actuators and computing nodes via cloud infrastructure or mobile apps and sharing of security credentials. The IoT has a worldwide network of smart devices which enables peoples or things to collect and exchange data. The IoT is characterized by an unprecedented set of heterogeneous, distributed, and intelligent things such as simple actuators, sensors, and RFID tags, as well as more complex devices such as computers, self-driving vehicles, and autonomous robots [1]. The Internet of Things allows people and things to be connected Anytime, Anywhere, with Anything and Anyone. "The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enable these things to connect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions". The term "Enterprise IoT" refers to devices used in business and corporate world. By 2019, it is estimated that EIoT for 9.1 billion devices [2].

The devices in IoT are based on various software and hardware platforms which belong from various different networks. The IoT structure should support and provide valuable services for such an heterogeneous networks. The devices in IoT infrastructures utilises different protocol for communicating with each other. The communication protocols differ according to the wired and wireless technologies. IoT infrastructure provides a common platform to integrate various protocols together for easy and safe communication in between them. But there is no standard are defined in IoT for various sort of protocols. The IoT infrastructure relates to speaking and hearing object in distributed environment where sensors are treated as speaking object and actuators are treated as hearing object. The speaking objects can be nodes of a dense distributed computing infrastructure which can be exploited to monitor and control activities in real-time in our everyday environment [3]. IoT devices have become an essential part of the life and are used in many areas as provided in below figure. IoT systems have applications across various fields through their unique identity and ability to be suitable in any environment. They boost data collection, automation, operations, and much more through their smart technology. The IoT infrastructure is growing faster and globe is becoming more smarter which helps in Information and Communication Technologies (ICT) like green radio-frequency identification, green wireless sensor network, green cloud computing, green machine to machine, and green data centres which contribute enabling green IoT infrastructure [4].

A. Consumer applications

The consumer application includes the connected vehicle, home, health and appliances with remotely monitoring capabilities. The things get connected with other in a worldwide network which are addressed uniquely and communicate with each other. Figure 1 shows various IoT applications.

Revised Manuscript Received on 30 March 2019.
***** Correspondence Author
Mr. Darshan Pradeep Pandit, Dept of Computer Science and Engineering, Walchand Institute of Technology, Solapur, India.
Dr. Sudhir Ranjan Pattanaik, Dept of Computer Science and Engineering, K L University, Vijayawada, India.

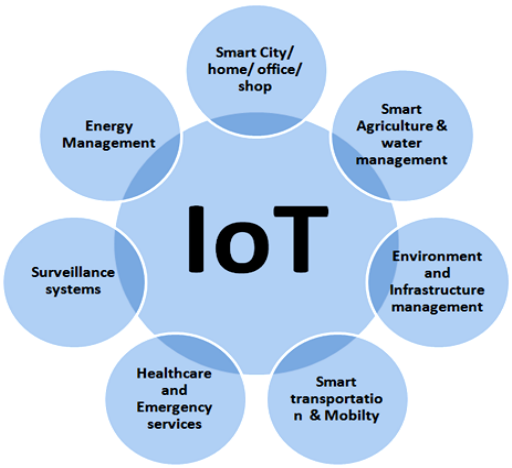

Figure 1: Applications of IoT

1. Smart City/ home & Enterprise applications

The smart home technology is a wide concept of home automation which can include switching on/off lights, cooling/heating air conditioners, playing media and security alarm systems. The business and corporate world will be totally dependent on IoT devices. The Smart Home comprises of many smart appliances like WIFI Router, Air Conditioner, Microwave oven, Refrigerator, Washing Machine, Heater, Iron, Dishwasher, Lights, etc which can be controlled and managed by the IoT infrastructure. Smart home connectivity services helps in providing the capabilities and functionalities required to connect the smart home controllers to the IoT infrastructure through smart home edge devices [5].

2. Environment and Infrastructure management

Infrastructure applications deals with monitoring and controlling operations in developing infrastructures like roadways, bridges, railway tracks, on- and offshore-wind-farms is a key application of the IoT. The IoT infrastructure helps in monitoring each and every activity or also helps to get any modification incurred in structural conditions and functional behaviour which helps in safety and risk management. IoT can help the infrastructure by saving cost, reducing time, providing quality work, reducing pen/paper work and increase in daily productivity. It can help in taking faster decisions and save money with Real-Time Data Analytics. Scheduling repair and maintenance activities in an efficient manner can be provide by IoT infrastructure. It can also coordinate the tasks between various service providers and users of infrastructure. IoT devices can also be used to control crucial infrastructure where “humans cannot work but IoT works” like opening and closing bridges to provide access to ships and vehicles. These infrastructures help in improving incident management and emergency calls coordination, and quality of services.

3. Smart Agriculture and Water Management System

Agriculture IoT in farming used to collect information on soil content, fertilizer required temperature, rainfall, humidity, wind speed, pest infestation. Further this information can be utilised for automating farming techniques [6]. This also helps in decisions making with improved quality and quantity. This IoT reduces risk and waste, and reduce time and effort required to manage crops. The IoT based Management System helps in managing and planning water usage. The Sensors are used to detect the water level and water flow is turned on/off automatically [7].

4. Energy management

A smart management on energy flow to between supplier and consumer by integrating smart meter to identify energy consumption and wastage. The Energy Management system is very helping for smart development of the cities which frequently requires analyzing IoT data from the heterogeneous interconnected network in order to optimize efficiency, comfort, safety, and quicker decisions. The devices in IoT infrastructure are based on Low power like Bluetooth, Zigbee, RFID, NFC, etc. The energy management comprises of managing of the low powered devices and lightweight process with optimized algorithm, rule and model for energy consumption. The energy management is used to construct a green and sustainable smart city [8].

5. Medical and Healthcare:

IoT infrastructure plays an important role in most sensitive area of healthcare and medicine. Smart analysis of various hospitalized patients with helps of monitoring sensors and wearable devices. Iot helps in providing quick services and diagnosis the patient in time. It provides real-time analysis of medical issues, telemedicine and computer-assisted smart transportation in case of emergencies. The Medical and Healthcare mainly aims in continuous monitoring quick treatment and consultation from medical experts from a distance. It is closely related with Safety-critical i.e. serious damage or loss of life due to any breakdown or trouble and Mission-critical i.e. treated as important part of business operation or an organisation, the breakdown or trouble may directly affect the business operations or organisation [9].

6. Transportation and mobility:

IoT also helps Smart transport management in assisting and finding direction towards destination. The smart transport and mobility management reduces problem of traffic jamming and ensure safe drive with help of sensors and smart information system. It helps in tracking current location of vehicle and monitors various infrastructures like road, tunnels, bridges, airports, crowded areas, etc. The IoT infrastructure allows interacting with other vehicles and providing technology for safe and sound mobility. It also allows sharing the transport system like cars, bicycle, etc. The smart Transportation and mobility can also assist with traffic signals, parking lots and roads anomalies [10].

B. Layered Architecture of IoT:

Figure 2 represent layered architecture of IoT which helps in connecting various devices at different layer. Also it enables the developer for designing and developing the applications at each layer. The white block is treated as user layer, Dark blue is treated as runtime layer and the light blue layer is treated as developer layer. This layer provides architecture for integrating and managing the devices in Iot Infrastructure at real time along with the security and safety [11].

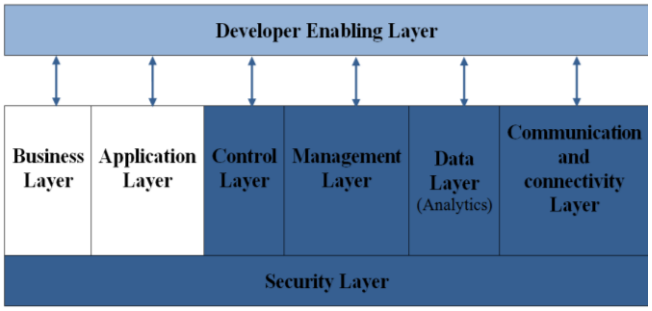

Figure 2: Intel Reference Architecture for IoT (Ref. [11])

1. Business Layer

The Business layer uses application layer in order to get access from all other layer. Business layer is related to the e-commerce management techniques used by any organisation or any educational institute to achieve business related goals. This business layer provides analysis of IoT infrastructure and Future development based on user or device report. The business layer plays an important role in managing the whole IoT infrastructure in which real time data recorded and analyzed to provide quality services and life time of the product or devices to the stakeholders [12]. This layer will be most helpful for software approach in developing the relationship between the applications and the devices in the IoT infrastructure and enable Quality of Services (QOS) guarantees.

2. Application Layer

Application layer is contains IoT specific applications which provide various different services to the stakeholders of IoT. The huge variety of applications are deployed in various fields like

- Smart City/ home/ office/ shop
- Smart Agriculture & water management
- Environment and Infrastructure management
- Smart transportation & Mobility
- Healthcare and Emergency services
- Surveillance systems
- Energy Management

The application layer enables interaction between stakeholders and the IoT devices. The applications are designed and developed as per user requirement. The applications can be developed in smaller modules and then it can be provided to the end user for verification and validation. Each and every unit of the applications should be thoroughly tested before the application is handed over to the end user.

In IoT infrastructure each sensor is associated with producing the data and an application to manage that data. With the IoT devices, applications are also growing rapidly which should be managed and controlled in order to avoid heavy load on the IoT infrastructure. The IoT can be also used to monitor elder behaviour for aged peoples who are categorized by some physical or cognitive disease and identify any behavioural change and analyze the risk associated with it. This helps in taking precautions for older peoples and improve the decision making process based on their behaviour [13]. The software approach provides a standard set of rules which allows to developers to develop standard and reusable applications.

3. Control Layer

The control layer maintains the set of policies for controlling and managing the IoT devices. This layer deals with hardware and software part of the IoT system and associated functions of it. The control layer is mainly responsible for identifying and assessing the interconnections of heterogeneous IoT network. It also helps in monitoring and controlling various interoperable device and its applications. This layer offer support to various layers of IoT which is the primary concern of software oriented. This layer also deals with various services and network related functions, which suggest when and from where to retrieve and deploy the data. The Object Oriented approach can be used for software design, classes and their generalization concepts which help in the behavioural characterization of the respective concepts [14]. The software approach helps in providing a significant way of retrieving and deploying the data in IoT infrastructure.

4. Management Layer

The management layer supervises end nodes of IoT. It is responsible identifying the devices and associated functions of IoT infrastructure. This layer deals with managing the devices which contains a management agent that emphasis communication between various connected devices in IoT infrastructure. The management layer provides various management functions related to Mission-Critical IoT, Security of transactions and massive data flow in IoT infrastructure. The software approach helps management layer in indentifying the attribute and functions of IoT devices so that devices can be handled properly and identify the uncertainty ranging from unknown device characteristics to emerging IoT data [15].

5. Data Layer

The data layer is responsible for managing massive data generated by various devices in IoT heterogeneous infrastructure. The data layer provides analysis and processing of data to various nodes present in IoT infrastructure. The data might be real time or time-critical, it can be computed either on edge or centrally on IoT cloud platform. The data layer is responsible for deciding and distributing the computation of data over IoT infrastructure. Now a day's if we IoT data come up with its Meta data like MAC address, timestamp, GPS location, and camera settings which will help in analysing and organizing the data [16]. This layer also plays an important role in classifying the data according to its type, size, efficiency, runtime and other various parameters. The software approach can provide various patterns and agile based modelling techniques for design, developing and deployment of IoT data as per user requirements. The data in IoT infrastructure is scalable for which scalable application design is required to integrate multi-input and multi-output applications [17].

6. Communication and connectivity Layer

The Communication and connectivity Layer provide smooth communication between various stakeholders and IoT devices in IoT infrastructure.

The IoT infrastructure consists of different communication protocol based heterogonous network and different technology used in that network. This layer flawless provides a platform for various IoT devices to communicate with other devices inspite of having different communication protocol [18]. The software approach provides a modelling technique to identify the protocol type and integrate into IoT infrastructure. It also helps in type of messages used for communication and offer priority based services.

7. Security Layer

The security layer is responsible for providing end to end security in IoT infrastructure. The security layer deals with hardware security, software security and enables secure communication between them. This layer is responsible for verifying various policy certificates, portfolios and authenticating user credentials. This layer helps in disabling malware, e-crime and manage privileges rights. The software approach provides the set of standards to enable security in IoT infrastructure, starting from requirement gathering phase to deployment phase.

8. Developer Enabling Layer

The developer enabling layer is responsible for deploying secure, interoperable and scalable applications which can be compatible for every layer in IoT. This layer works with all other seven layers in order to maintain reliable communications between application and stakeholders of IoT infrastructure. This layer utilises available API's, SDK's and DEV tools to develop the applications as per the user requirements. The software approach can reduce the design and development time by providing reusable object. The software approach enables the developer to design and implement application based on design documentations and use cases. It also helps in maintaining the test case and test scenarios which helps the further developer to follow the same and update it.

II. LITERATURE SURVEY:

Larrucea[1] focused on several economic and technical issues and suggested to avail standard software engineering methodologies for IoT. He also suggested that past software engineering techniques can be upgraded for the challenges of today's IoT. Rethinking is on the configuration management is required in the context of the extremely dynamic, continuously reconfiguring systems which are characteristic of the IoT. He stated to adopt agile practice and methodologies in developing and designing the IoT infrastructure. The IoT infrastructure require a suitable guidance to engineer the new generation of scalable, highly reactive, often resource constrained software systems characteristic of the IoT. Also Spinellis et al. elaborated progress from ENIAC (Electronic Numerical Integrator and Calculator), EDVAC (Electronic Discrete Variable Automatic Computer) and milestone for modern computing. It involves multiple stakeholders, such as cities, private residences, large office buildings, and mobility applications. The Requirements linked with control, privacy, and reliability might speak about design decisions that will be at odds with IoT nodes' processing capacity, power budget, bandwidth, and ubiquity. Courtais et al. stated that Software and hardware heterogeneity are both strength and a big challenge of IoT systems. Researchers have to exploit the power of models and model transformations to guarantee the runtime preservation of quality attributes both in isolation and in combination. MC-IoT systems will need more powerful, fully automated mechanisms for selecting the most suitable configuration, as well as self-reconfiguration capabilities. In this paper the author highlighted the challenge in coordinating multiple stakeholders with their conflicting interest regarding IoT.

Even Kotronis[9] stated that the real-time monitoring process is safety-critical. The fault isolation is also a safety-critical like Faults in an application / device must not propagate to other. Communications between devices should be confidential. Well-known network with respect to security protocols and software suites can be employed. Also Cerf[31] focused his attention to the fragile and interdependent future and Concerns for safety, security, privacy, and control that must be assuaged by systematic analysis of increasingly complex use scenarios. The author also suggest like an immense attention and efforts have to be expended or modelled in order to improve the resistance of devices in IoT which are vulnerable various forms of attack and failure. This expansion should be concern with safety, security, privacy, and control must be satisfied by systematic analysis and modelling of increasingly complex use scenarios of IoT infrastructure. Ciccozzi[20] introduced that the software community is to provide application developers with the proper level of abstraction to interact with IoT platforms. He described IoTVar middleware technology that manages interactions between end-user applications and IoT platforms through IoTVar proxies. The author stated that software developer should be enabled to easily declare IoT variables in their applications which help in appropriate abstraction level to end-user applications, discovery and identifying Internet of objects, storage of contextual data produced by the objects, contextual data management and data analysis. Even Sherwood[41] said that the test designs must accommodate system complexity and size, as well as diverse objectives. Constraint challenge is generating test cases that lead to a particular expected state or class of expected results. As per the author constraints like class pair's equivalence should be verified according to univariate and multivariate equivalence with respect to the class boundaries. Also Zambonelli[42] stated that a common set of abstractions, models, and methodologies are still missing, a unified approach should be developed for Analysis, Design, development of IoT devices like Simple RFID tags or Bluetooth beacons, based on low-cost communication protocols. The author also suggests a need of software infrastructures for bridging the gap of interoperability, indentifying common semantics between the devices and group formation and coordination, context awareness and self-adaptation. This can be adopted by implementing an middleware infrastructure and programming model or agent-based model. Here Martın[34] suggested that IoT devices cannot be configured at once in the beginning, but also users must reconfigure them as their habits and needs change which may be addressed by developing software capable of adapting its behavior to the people's needs. As IoT devices are produced by various manufacturers, each with their own interaction model.

The strategies should be developed for one user and then it should be applied for various users which help in developing the services in order to exchange the information between various entities. Broring[43] focused on IoT platforms that act as closed silos with a very narrow application. It promotes their specific interface and data formats and typically restrict communication to those formats. This fact is preventing a broadly accepted IoT ecosystem to emerge. To activate the ecosystem, BIG IoT should follow an approach of openness towards the IoT developer community which include an open development of the API and releasing the developed software as open source. Also Chan et al. claimed that growing applications with new devices or behaviors, or extending the existing infrastructure with new applications should involve redesign and redeployment. We must find a new ways for devices and software to interact and share valuable insights by indentifying the user context from the sensors and applications. The today's IoT infrastructure system demands a novel and scalable software infrastructure which require a data analysis occurring at each layer in our system. Even GirayBedir[18] stated that an improvement area can be the development of a system engineering kernel to cover hardware and communication aspects of IoT systems. Scrum practice should be complemented with a practice to specify requirements, such as use case, user story, or any other practice. He proposed an initial practice library, which can be used to develop and/or tailor project-specific IoT system development methods. Krishna[29] identified conceptually modelling of data, control and process flow for IoT-driven smart applications is more challenging. Eg sensors built for the Smartphone application and Smartphone's are prone to energy-related issues. The author also stated that ER model serves as a meta-model template for building IoT applications and solutions. Here Kettunen[37] aims to recognize the design principles of future software organizations and point out how most decision-making in companies will be more and more software-related when companies focus on software based on following key values

- Value Economy
- Real-Time Business
- Employee Satisfaction
- Customer Satisfaction
- Customer Retention
- Service Availability

He stated that new kind of structures and roles / competencies may be needed to support agile and flexible development needs and goals with respect to IoT. Also Schmid[25] stated that Platform providers that use off-the-shelf platform solutions, and thus have no access to the source code of their platform. Constrained device-level platform providers need infrastructure-level support to overcome the availability and cost limitations of such platforms. He focused on decision like marketplace functionality on an IoT resource exchange, Consumers access IoT resources directly on the provider. Providers and consumers can participate on multiple marketplaces. Author also suggested some of the use case and requirement for Use Cases and Requirements for

- Core technology
- Developer support
- Exchange of resource offerings
- Charging and billing
- Non-functional requirements

He even stated that interoperability enables the cross-platform and cross-domain application deployments in IoT infrastructure platforms and marketplaces to share and monetize IoT resources. Also Morin[19] suggested that there must be a standard for IoT which combine things readily available in the environment with some generic, application-specific, and legacy things. Not much research has been addressed on distribution over a large range of processing nodes & high heterogeneity of the processing nodes and the protocols used between them. The important software engineering challenges remain, particularly regarding software deployment and updates and reliable, predictable sharing of computational resources and devices among IoT applications. Franzago[17] were also concern for methods and techniques where multiple stakeholders manage, collaborate and are aware of each others. Software production is more and more subject to globalization, with teams required to work distributed and with fast pace, and with stakeholders coming with different potentially conflicting concerns, As in IoT infrastructure each and every stakeholder will come with its own type of model which is specialized to certain analysis or code generation. Truong[15] stated that there is a lack of novel ways to model and prepare the right infrastructural elements covering requirements for testing emerging uncertainties. The various parameters of uncertainties, test strategies, costs and underlying cloud providers, is just at an early stage that needs to be addressed in the future. Here Venkatesh[22] interpreted that applications should scale well both with the number of inputs and to the available computing environment. As IoT applications operate in a dynamic environment in which sensors and actuators move through an application's domain. The aims to identify user interaction with an device and determine whether using this device was flexible at a given time, the optimization for each is crucial to the real-life context-aware applications. Ciccozzi[20] stated that Software must provide assurance regarding system properties such as safety, reliability, and fault tolerance. The critical quality attributes of software-intensive systems, such as reusability, flexibility, and interoperability. He highlighted a lack of overall architectural models and methods. Even Einarsson[5] all cloud-enabled devices should have a uniform communication interface. In order to achieve it, we would need to select a range of supported cloud enabled devices, study their interfaces, and adjust transformation templates accordingly. As there is increasing demand for smart home connectivity from controlling the home temperature, to switching light bulbs, controlling the window shades and pet feeders. Smart home control systems like Amazon Alexa and Google. Also Houliotis[35] claimed that there is a need for an innovative architecture approach that allows components from different manufacturers to be integrated, paying particular attention to the system's mission, safety, and security. At first time if right mission-critical elements are applied then a successful mission can be achieved. Usually when there is maturity in the applied mission-critical elements.

The second attribute is when enough knowledge is accumulated to allow for the prediction of a mission outcome to be more accurate. At the present there is no any current development activities employed for mission-critical systems. Exman[14] introduced that the Software Engineering has two fundamental implications like software is far away from the machine which may be a real or a virtual machine; software understanding by human or robotic stakeholders are either a developer or a user, is at the heart of high quality design of any software system. The formalization of the principles behind Conceptual Integrity in an axiomatic fashion, provide a deeper justification for the algebraic operations found in the Linear Software Models. It also enables calculations of quantitative criteria for Conceptual Integrity. The highlighted Orthogonality i.e. individual functions should be independent of one another. Propriety i.e. a product should have just the functions essential to its purpose. Generality i.e. a single function should be usable in many ways. Also Lippi[3] suggested about Key Research challenges at the level of software engineering models, middleware technologies, user involvement, control and understandability, security. He also stated that IoT systems require identifying novel software engineering abstractions and novel approaches to modelling and design. Such need is even more compulsive in the speaking object scenario. The author suggested that the outputs of multiple sensors where each sensor has some specific outlook on the surrounding world which are combined together to form a more comprehensive understanding. Maamar[45] also contributed by stating that diversity of things development technologies and communication standards, end-users reluctance and sometimes rejection due to privacy invasion, limited number of killer applications that would demonstrate their necessity and justify their return-on investment, lack of an IoT-oriented software engineering discipline are multiple obstacles are slowing down IoT expansion and adoption. The author also stated about Agentification that should make devices very responsive to their surroundings, which satisfies users requirement and identify collaboration between various devices. The author highlighted regarding business and social norms which are strictly application dependent should achieve the proper and secure communication between the devices.

III. ISSUES IN IOT

There are several issues identified in IoT after surveying the broad literature available, as shown in figure 3.

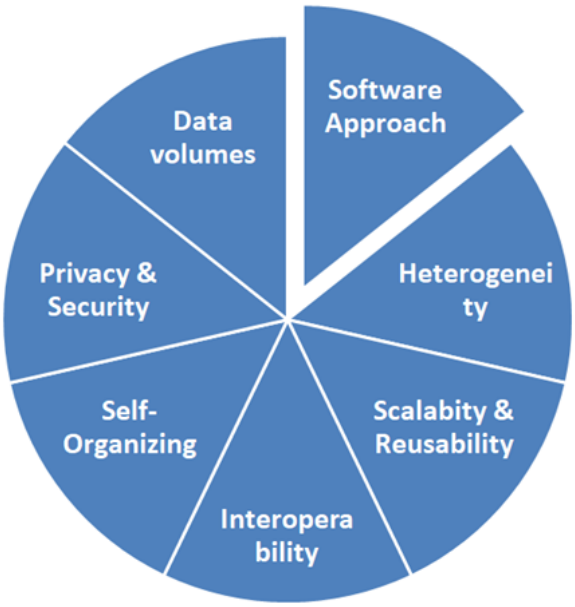

Figure 3: Issues in IoT

A.Heterogeneity:

The IoT devices are based on different hardware and software platforms and belong from any networks. The different IoT devices get connect to other IoT devices via available network. All IoT should prevail common standards or mechanism for easy and safe communication in between them (Brice Morin et al., 2017). The heterogeneity content like wearable and house sensors varies in source, data, accuracy, format, size, etc which belongs to various platform and heterogeneous network. IoT systems involve distributed architectures in which sensors and end-user applications interact through IoT infrastructure platforms deployed on the cloud network or at the node edges. IoT variable should be easily defined and discovered for objects for regular updates [20]. The figure 4 provides heterogeneous architectures of IoT are contains various Wireless Fidelity network, Mobile Communication Network, Wireless Sensor Network, Vehicular Network and Wireless Mesh Network which should provide various valuable and convenient services. Each network comprises of sensors and devices which are responsible transferring and receiving information. Each sensor and devices come with their own communication protocol the heterogeneous network of IoT infrastructure should be capable of understanding the nature of device and provide quality service along with security to the stakeholders. The most important thing is to fetch or sense the data from smart devices in order to gather information which is distributed over various environments. Once the data is sensed and gathered from various devices then the data it is stored on the cloud or any edge platform. This is routed through the network layer which contains efficient topology and various routing techniques. At the cloud computing act as a interface between application layer and sensing nodes. The application layer allows various devices to communicate with each other under various network environments like Wireless Fidelity network, Mobile Communication Network, Wireless Sensor Network, Vehicular Network and Wireless Mesh Network [21].

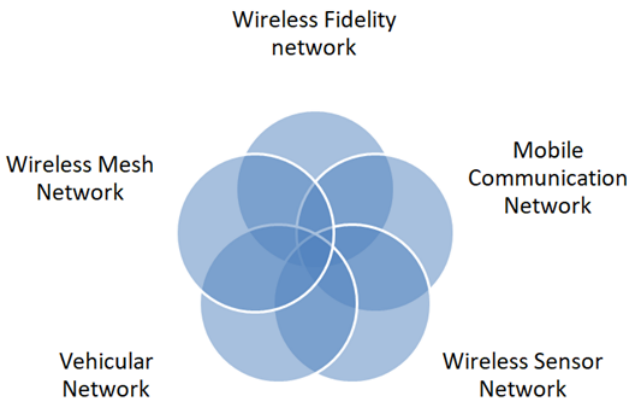

Figure 4: Heterogeneous network of IoT infrastructure

B. Scalabity:

As we know IoT comprises lots connected devices and inter connected network. IoT infrastructure should provide services to all the connected devices by understanding the nature of the device. It should be scalable for large and small environment. The applications should also scale well both with the number of inputs and to the available IoT infrastructure environment. The sensors and actuators will be moving in a application domain with respect to the changing environment of IoT where each application is responsible for maintaining its own data and user interactions. In scaling, handling this type of applications should cover more number of users and a larger physical or virtual space effectively in the existence of other embedded devices for sensing or actuation, data aggregation, and computation with respect to growing nature of IoT infrastructure. In IoT distributed network the scaling definition can be extended to bind and measures the performance of a system under two conditions firstly when there is a change in number of computational nodes for an application i.e known as strong scaling and Secondly when there is a change in the amount of input data i.e. known as load scaling [22].

C. Reusability:

Different function, solution and the devices must be reused for the construction of IoT infrastructure which helps in developing sustainable software's [23]. The reusability helps in forming new patterns and design for IoT infrastructure. The most important factor in the academics and industries is reusing the components or objects instead of creating new one which save stakeholders time and efforts. In IoT infrastructure consist of huge number of sensors and devices and it is increasing day-by-day. These devices create their own new instances which makes the IoT infrastructure even more complex. Maintaining the relationship between various devices and reusing them requires clear understanding of IoT infrastructure. The reusability of object or device is categorized into horizontal layered architecture and vertical layered architecture platforms. In horizontal platform, the reusability of objects or software should be applied in IoT infrastructure in order to minimize the storage space, recreation of new objects, duplications of objects, etc which helps in increasing the Scalability. In vertical platform used to provide modularity service which helps in making small modules and recombine at the destination, future development, easily available, and scalability of IoT services. Proper design and use-cases should be well implemented in order to reuse the object and device functionality [24].

D. Interoperability:

Various types of included in IoT infrastructure containing different sort information and possess different types of processing, bandwidth and communication capabilities. IoT infrastructure should be capable of providing easy means of communication and connectivity between these devices. The interoperability should allow cross-platform and cross-domain application developments by using existing platform. It should also allow marketplaces to share and monetize IoT resources [25]. The cross-platform interoperability is one of the major issues in IoT infrastructure which relates to the heterogeneous network and their functions like clouds services, edge services, data centres, etc. This interoperability includes various protocols for device communication, type of data (formats), deployment mechanisms, and performance factor of each device. Proper services and platform should be developed for providing interoperability service deployment. There should be some middleware technology which bridge the gap between various functions of IoT devices and IoT network which helps the stakeholder to work on multiple platforms with single device [26].

E. Self-Organizing:

The Smart devices should be self configuring and should be adopted according to the dynamic nature of IoT infrastructure. Devices should identify each other by their activity and behaviour. IoT infrastructure has made a huge advancement in different areas which include also development of new heterogeneous network architectures, platforms and applications. Iot should allow self-organization of the network in case of disaster or any failure for further communication of various sensors and devices present in the network to achieve common goals. The self-organization relates to the understanding of the system and get adapted to the system. The self-organization consist of some intelligence with respect to discovering the adjacent network and device, controlling medium access and path discovery between various network nodes, local connectivity and managing recovery of services [27].

F. Privacy & Security

Privacy & Security are the most important concern with IoT and its infrastructure as data is scattered all over the network. It should be handled properly and security should be maintained with respect to four generic layer of IoT i.e. Perception layer, Network layer, Middleware layer, Application layer. As we all know most of device use air medium for their communication which are accessible by all and hence they are more vulnerable for various attacks. It should also provide security and privacy for all technologies ranging short range to wide which are embedded in IoT infrastructure [28].

G. Data volumes:

The devices in the IoT infrastructure produce huge of amount of data. Managing and mining large amount of data information to provide valuable services to the stakeholders is a challenging task to the IoT infrastructure. The data may be of any type like structured, unstructured, massive, scalable etc. The storage and processing of data should be distributed properly in local and wide area network. The Big IoT data should not hamper the performance of the IoT infrastructure. IoT is a sensor which captures the data from sensors after that pre-process the captured data to store and load it to the data, or transfer the data to a data store. Understanding the data and control flow which presides over sensor data to IoT end user is a big problem. Hence it becomes more challenging task for modelling of data, control and process flow for IoT-driven smart applications, particularly when exception occur while execution [29].

H. Software Approach:

The design and development of sensors and actuators for IoT infrastructure are as per developer convenience. These devices consist of minimal functions. The developer designs the product as per the market strategies which do not contain any fault tolerance mechanism. No proper support system for IoT infrastructure developed. There should be proper set of standards for design and maintenance of IoT devices. Robust and flexible applications have to be built in order to deal with complex IoT heterogeneous infrastructure. The software approach should be able to reproduce the organisation structures and patterns in case of failure [30]. It becomes an ethical responsibility of the designer of the IoT device who are populating IoT infrastructure need to be aware of its diverse effects of IoT device interactions and about the companies which marketing the device and its services often bared by the end user customers for their failures [31]. The IoT infrastructure should involve restricting the setup of IoT devices and systems to walled gardens with strictly defined standards, processes, and compliance testing [32].

IV. SOFTWARE ORIENTED APPROACH FOR IOT:

In IoT infrastructure environment, heterogeneity is combined with both software and hardware. The devices in IoT infrastructure possess extremely robust application which should be able to tackle the problem like interoperability, heterogeneity, privacy, security, etc. We require software infrastructures for adhering interoperability operations, identifying Common semantics, network path discovery and grouping various devices, maintaining coordination between devices and the IoT infrastructure, identifying the context or nature of the devices and adopt the behaviour accordingly. The data analysis will occur at each and every layer of IoT infrastructure system which helps in extracting device context and identifying its behaviour, this requires a novel and scalable software infrastructure [33]. IoT devices are developed by different manufacturers along with their own interaction model, Context-Oriented Programming (COP) enables set of rules for software developers to setup the behaviour of the applications and activating or deactivating certain behaviours or functionalities based on their contextual information [34]. The software developer must specify and approve the criticality level of data at each layer which can be varied based on the application and technical specification related to user and system requirements. There is an need of innovative unified framework to describe and guide Mission-Critical Systems development leading to the mission success [35]. The Software oriented approach enables software developer to easily declare and integrate IoT variables in their applications. It is also used to identify the number of event generated by the device in IoT infrastructure and process accordingly with hep of Event Processing language [36]. The software approach used to evaluate the success of an organization based on benefit provided by a good or service, providing real time service, satisfaction of employee, customer satisfaction and availability of service whenever required. The step by step changes have to done and application should be delivered to the end user, IoT solutions have to be developed based on the feedback of the stakeholders. In order to gain goodwill and market need, users of IoT should be always satisfied [37]. The software approach must guarantee system properties in terms of safety, reliability, and fault tolerance with a systematic approaches, methods, models, and tools for real-world applications and solutions [38]. The organisation gets benefited from software approach ecosystem which share risks and costs associated with a network and their partners. This employs in managing the organisation by making quick decisions [39]. While making decision in regarding IoT devices and applications which integrated together, the IoT infrastructure must consider both functional and non-functional requirements in service composition developed with respect to software product line [40]. In order to obtain control, privacy, and reliability in IoT infrastructure, strict rules and standardization must be followed acquiring new adoption layer. Also processing capacity, power budget, bandwidth, and ubiquity must be considered while designing and constructing with respect to IoT system. The most important thing to consider regarding regular corrective and perfective maintenance and updating the system because vendors may change or switch to new system or business may go out over time and the user has to suffer the problem. In the IoT infrastructure many diverse heterogeneous devices work together which fails quality of life either at design time or runtime so there is a need of new software engineering approaches to be envisioned. Mission-critical IoT (MC-IoT) systems are based on run-time environment which focus on high-level abstraction, collaborative development, automated mechanisms, reusability, Dependability, safety, security whose failure may lead to significant economic, human, or environmental losses hence this system should be handled carefully with standard software engineering approach. The test design process in software approach provides functional dependencies between IoT devices and also improves accuracy, flexibility, control and automation [41]. The IoT infrastructure functionalities derive from the combining variety of things and variety of users and stakeholders which requires a new way to identify and establish a relationship among device and device, devices and humans and to coordinate their activities with each other.

The requirement gathering should be Policies, Goals, and Functions based and also they should be categorised locally and globally [42]. The software engineering approach also provide Interoperability Patterns interoperability with both syntactically and semantically so that device multiple platform would interact with each other without any interferences. These patterns can be reused and services can be composed together for easy assimilation of data from diverse platforms. The software engineering approach permits data providers and consumers to utilise same vocabularies for smart object, sensor, measurement, and so on [43]. The modern software development approach consist of collaborative teamwork and modern methodologies which helps in analysing the code written for devices, quality of code, evaluation of projects assigned and delivery of products [44]. The software oriented approach for IoT devices is a serious issue, as IoT devices are increasing tremendously day by day, these devices should be managed and controlled. The software oriented approach also ensures that the outcomes of these device operations are beneficial to the surroundings. It can used to categorize the IoT devices according business norms and social norms which helps devices and stakeholders with easy way of communication [45]. The past software engineering techniques and models can be harnessed and adapted to the challenges of today's IoT. The management challenge for a software engineering approach is to coordinate multiple stakeholders with conflicting interests, where multiple stakeholders may be cities, private residences, large office buildings, and mobility applications, etc [46]. After surveying various research papers, we have identified that 60 percent of the people talking about the need of software engineering approach for IoT infrastructure. Below table represent different issues of IoT addressed by various authors, Where Y depicts "Yes" and N depicts "No".

Table 1: Highlighted Issues addressed by Various Authors

Author	Interoperability	Reusability	Scalabity	Security	Privacy	Data Volume	Heterogeneity	Self-Reconfiguring	Software Approach
[1]	Y	Y	Y	Y	Y	N	Y	Y	Y
[3]	N	Y	N	Y	N	N	Y	Y	Y
[5]	Y	N	Y	Y	N	Y	Y	N	Y
[9]	Y	N	N	Y	Y	N	N	N	Y
[14]	Y	N	N	N	N	N	N	N	Y
[15]	N	N	N	N	N	Y	Y	N	Y
[17]	Y	N	N	N	N	N	N	N	Y
[18]	N	Y	Y	N	N	N	N	N	Y
[19]	Y	Y	N	N	Y	N	Y	N	Y
[20]	Y	Y	N	N	N	N	Y	Y	Y
[22]	N	N	Y	N	N	N	Y	N	Y
[23]	N	Y	N	Y	Y	N	Y	N	Y
[25]	Y	Y	Y	N	N	N	Y	N	Y
[25]	Y	N	N	Y	Y	N	Y	N	Y
[29]	Y	N	N	N	N	N	N	N	Y
[31]	N	N	N	Y	Y	Y	Y	N	N
[32]	Y	Y	N	Y	Y	Y	N	N	Y
[33]	Y	Y	N	N	N	N	Y	N	Y
[35]	Y	Y	N	N	N	N	N	N	Y
[37]	Y	Y	Y	N	N	N	N	N	Y
[38]	Y	Y	Y	Y	Y	N	N	N	Y
[41]	N	N	N	N	N	Y	Y	Y	Y
[42]	Y	Y	N	N	N	N	N	N	Y
[43]	Y	N	N	N	N	N	Y	N	Y
[45]	Y	N	N	Y	Y	N	Y	N	Y

V. SUMMARY

In this paper we have highlighted various issues of IoT devices like Interoperability, Reusability, Scalabity, Security, Privacy, Data Volume, Heterogeneity, Self-Reconfiguring and Software Approach. This paper also gives precise view and the need of novel software engineering approach for IoT devices.

The software engineering approach for IoT helps in improving the quality of the service and application by reducing the inherent inconsistency and complexity of IoT infrastructure and promoting the reuse of software and hardware components.

REFERENCES

1. Xabier Larrucea, Tecnalia, Annie Combelles, Inspearit, John Favaro, Intecs, Kunal Taneja, Google "Software Engineering for The Internet Of Things". IEEE Software, 2017.

2. link: https://en.wikipedia.org/wiki/Internet_of_things
3. Marco Lippi, Marco Mamei, Stefano Mariani, Franco Zambonelli, "Coordinating Distributed Speaking Objects", IEEE, 2017
4. CHUNSHENG ZHU, VICTOR C. M. LEUNG "Green Internet of Things for Smart World", IEEE, 2015.
5. Atli F. Einarsson, Patrekur Patreksson, Mohammad Hamdaqa, Abdelwahab Hamou-Lhadj, "SmartHomeML: Towards a Domain-Specific Modeling Language for Creating Smart Home Applications", IEEE, 2017
6. Zeinab Kamal Aldein Mohammed, Elmustafa Sayed Ali Ahmed, "Internet of Things Applications, Challenges and Related Future Technologies", WSN, 2017.
7. Sayali Wadekar, Vinayak Vakare, Ramratan Prajapati, Shivam Yadav, Vijaypal Yadav "Smart Water Management Using IOT", IEEE, 2016.
8. Chinmaya Mahapatra, Akshaya Kumar Moharana, Victor C. M. Leung, "Energy Management in Smart Cities Based on Internet of Things: Peak Demand Reduction and Energy Savings" I, Sensors 2017.
9. Ch. Kotronis, G. Minou, G. Dimitrakopoulos, M. Nikolaidou, D. Anagnostopoulos, A. Amira, F. Bensaali, H. Baali, H. Djelouat, "Managing Criticalities of e-Health IoT Systems", IEEE, 2017
10. Ricardo Faria, Lina Brito, Karolina Baras, José Silva "Smart Mobility: A Survey", IEEE, 2017.
11. White Paper: "Architecture Specification White Paper Internet of Things (IoT)", The Intel IoT Platform.
12. Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, Hindawi, 2017.
13. Almeida A, Fiore A, Mainetti L, Mulero R, Patrono L, and Rametta P, "An IoT-Aware Architecture for Collecting and Managing Data Related to Elderly Behavior", Wireless Communications and Mobile Computing, Hindawi, 2017
14. Iaakov Exman and Phillip Katz, "Conceptual Software Design: Algebraic Axioms for Conceptual Integrety", SEKE, 2017
15. Hong-Linh Truong, Luca Berardinelli, Ivan Pavkovic, Georgiana Copil, "Modeling and Provisioning IoT Cloud Systems for Testing Uncertainties", ACM, 2017
16. Hsin-Yi Tseng, Cheng-Ting Lee, Pai H. Chou "IoT Metadata Creation System for Mobile Images and its Applications" IEEE 2017.
17. Mirco Franzago, Davide Di Ruscio, Ivano Malavolta and Henry Muccini, "Collaborative Model-Driven Software Engineering: a Classification Framework and a Research Map", IEEE, 2017
18. Görkem GirayBedir Tekinerdogan, Eray Tüzün, "Adopting the Essence Framework to Derive a Practice Library for the Development of IoT Systems", Springer, 2017
19. Brice Morin, Nicolas Harrand, Franck Fleurey, "Model-Based Software Engineering to Tame the IoT Jungle", IEEE, 2017
20. Ciccozzi, Crnkovic, Di Ruscio, Malavolta, "Model-Driven Engineering for Mission-Critical IoT Systems", IEEE, 2017
21. Tie Qiu, Senior Member, Ning Chen, Keqiu Li, Mohammed Atiquzzaman, Wenbing Zhao, "How Can Heterogeneous Internet of Things Build our Future: A Survey" IEEE, 2018.
22. Jaggannathan Venkatesh, "Scalable Application Design for the IoT", IEEE, 2017.
23. Courtais, Taconet, Conan, Chabridon, Gomes, Calvacante, Batista, "IoTVar to transparently handle interactions between applications and IoT platforms", Acm, 2017
24. Muhammad Aslam Jarwar ID , Muhammad Golam Kibria ID , Sajjad Ali ID and Ilyoung Cho, "Microservices in Web Objects Enabled IoT Environment for Enhancing Reusability", Sensors 2018.
25. Stefan Schmid, Arne Bröring, Denis Kramer, Sebastian Käbisch, Achille Zappa, Martin Lorenz, Yong Wang, Andreas Rausch, Luca Gioppo, "An Architecture for Interoperable IoT Ecosystems", Springer, 2017
26. Hong-Linh Truong, "Towards a Resource Slice Interoperability Hub for IoT", IEEE,2018.
27. Arjun P. Athreya and Patrick Tague, "Network Self-Organization in the Internet of Things", IEEE, 2013.
28. Zejun Ren, Xiangang Liu, Runguo Ye, Tao Zhang, "Security and Privacy on Internet of Things", IEEE, 2017.
29. P. Radha Krishna, Kamalakar Karlapalem, "Data, Control, and Process Flow Modeling for IoT Driven Smart Solutions", Springer, 2017
30. Markus Schattena, Jurica Sevab, Igor Tomicica, "A roadmap for scalable agent organizations in the Internet of Everything", Journal of Systems and Software, 2016
31. Vinton G. Cerf, "A Brittle and Fragile Future", ACM, 2017
32. Diomidis Spinellis, "Software-Engineering The Internet Of Things", IEEE, 2017
33. Christine S Chan, Michael H Ostertag, Alper Sinan Aky¨urek, and Tajana Simuni´c Rosing, "Context Aware System Design", SPIE, 2017
34. Daniel Flores Martın in University of Extremadura, Caceres, Spain, "Meeting IoT Users' Preferences by Emerging Behavior at Run-Time?", Synopsis, 2017
35. Kyriakos Houliotis, Panagiotis Oikonomidis, Periklis Charchalakis, Elias Stipidis, "An Efficient Approach to Designing Mission-Critical Systems", IEEE, 2017
36. L. Gutierrez-Madronal, Inmaculada Medina-Bulo, Juan José Domínguez-Jiménez, "IoT-TEG: Test event generator system", Journal of Systems and Software, 2017.
37. Petri Kettunen, Maarit Laanti, "Future software organizations – agile goals and roles", Springer, 2017
38. Federico Ciccozzi, Davide Di Ruscio, Ivano Malavolta, Patrizio Pelliccione, and Jana Tumova, "Engineering the Software of Robotic Systems", IEEE/ACM, 2017
39. George Valençaa, Carina Alves, Slinger Jansen, "Strategies for managing power relationships in software ecosystems" Journal of Systems and Software, 2018.
40. Mahdi Basharia, Ebrahim Bagheri, Weichang Dua, "Self-adaptation of service compositions through product line reconfiguration", Journal of Systems and Software, 2018.
41. George B. Sherwood, "Embedded functions for test design automation", Springer, 2017
42. Franco Zambonelli, "Key Abstractions for IoT-Oriented Software Engineering", IEEE, 2017
43. A Bröring, S Schmid, C Schindhelm, A Khelil, S Käbisch, D Kramer, D Phuoc, J Mitic, D Anicic, E Teniente, "Enabling IoT Ecosystems through Platform Interoperability", IEEE, 2017
44. Claudia Raibulet and Francesca Arcelli Fontana, "Collaborative and Teamwork Software Development in an Undergraduate Software Engineering Course", Journal of Systems and Software, 2018.
45. Zakaria Maamar, Noura Faci, Slim Kallel, Mohamed Sellami, Emir Ugljanin, "Software agents meet internet of things", WILEY, 2017
46. Che-Wei Chang, Chun-Yi Liu, Chuan-Yue Yang, "Energy-efficient heterogeneous resource management for wireless monitoring systems", Journal of Systems and Software, 2017.

AUTHORS PROFILE

Mr. Darshan Pradeep Pandit, received M.E degree in Computer Science & Engineering in 2013 from Walchand Institute of Technology, Solapur, Maharashtra,, India and pursuing the Ph.D in Computer Science and Engineering in K.L University, Vijayawada, Andhra Pradesh, India. He is doing his Ph.D work under the guidance of Dr. Sudhir Ranjan Pattanaik, Professor, Dept of CSE, K L University, Vijayawada. Also he is working as an Assistant Professor at Dept of Computer Science and Engineering, Walchand Institute of Technology, Solapur, MH.

Sudhir Ranjan Pattanaik received PhD degree from Chang Gung University, Taiwan, under computer science stream in electrical engineering Department in 2017, Master of Science in mathematics from Sambalpur University, India in 1999, Master of Philosophy in mathematics from Berhampur University, India in 2002, Master of Technology in Computer Science from the Utkal University, India in 2006 and currently working as a professor in department of Computer Science and Engineering in K.L University, Vijayawada, Andhra Pradesh, India. His research interests include the performance analysis of Wireless Sensor Network, MAC protocol design, M2M communications, VNET, Smart home/city applications and Internet of Things.