ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

SOA Network Security for IOT Using Sensors as a Service

T.V.Lakshmi Sukrutha[1], S.Sri Lakshmi Anusha [2]

Assistant Professor, Dept. of CSE, Methodist College of Engineering and Technology, Hyderabad, Telangana, India [1]

Assistant Professor, Dept. of CSE, Methodist College of Engineering and Technology, Hyderabad, Telangana, India[2]

ABSTRACT: The Internet of Things (IoT) is increasing the connectedness of people and things on a scale that once was unimaginable. Connected devices outnumber the world's population by 1.5 to 1. The pace of IoT market adoption is accelerating because of, Growth in analytics and cloud computing, increasing interconnectivity of machines and personal smart devices and the proliferation of applications connecting supply chains, partners, and customers. When IOT app is deployed in global scale to millions of users simultaneously through Internet, it is leading to many Security challenges and Issues. In this paper we are going to discuss How Security has become an Issue in IOT and how IOT devices of different platform Applications can communicate through SOA and provide security through SOA Network Access control in order to Authenticate Users.

KEYWORDS: IOT, Sensors, SOA, Sensors as Service, SOA Network Security for IOT

I. INTRODUCTION

Internet of Things represents a general concept for the ability of network devices to sense and collect data from the world around us, and then share that data across the Internet where it can be processed and utilized for various interesting purposes. The physical objects that are being connected will possess one or more sensors. Each sensor will monitor a specific condition such as location, vibration, motion and temperature. In IoT, these sensors will connect to each other and to systems that can understand or present information from the sensor's data feeds. These sensors will provide new information to a company's systems and to people [1].IPv6's huge increase in address space is an important factor in the development of the Internet of Things. The address space expansion means that we could assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths. In other words, humans could easily assign an IP address to every "**thing**" on the planet. People have been more connected with the Emergence of Smart Devices, where everything was controlled by one touch on the device. An increase in the number of smart nodes, as well as the amount of upstream data the nodes generate, is expected to raise new concerns about data privacy, data sovereignty and security.

Internet of Things - things with microprocessors and operating systems. This means many millions of possible security points that need to be guarded against hackers as much or even more than the large server farms. It describes a network of physical objects that connect to each other through the internet. Objects, or 'things' can transfer information wirelessly without requiring human interaction. A 'thing' can be any object that can be assigned an IP address and provided with the ability to transfer data over a network. the IoT is a network connecting things to things for achieving intelligent identification and management of the items in a broad sense; it can be seen as a fusion of the information space and physical space. Through that way, everything is digitized and networked, which results in realizing an efficient information interactive mode between items, items and people, and people and environment. After that, various diversities of information are merged into social networks and integrated into human society in a higher realm. For realization of information fusion in the IoT, the middleware technology is suitable to be adopted as a concrete solution [2].

II. IOT AND SENSORS

The Internet of Things is governed by connected devices embedded with sensors .From a technology perspective, the IoT is being defined as smart machines interacting and communicating with other machines, objects, environments and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

infrastructures, resulting in volumes of data generated and processing of that data into useful actions that can "command and control" things and make life much easier for human beings. The types of sensing nodes needed for the IoT vary widely, depending on the applications involved. Sensing nodes could include a camera system for image monitoring, water or gas flow meters for smart energy, radar vision when active safety is needed, RFID readers sensing the presence of an object or person, doors and locks with open/close circuits that indicate a building intrusion or a simple thermometer measuring temperature [3].

If we categorize Sensors into groups, we will be able to name at least 10 distinct groups. This includes sensors that have been built on Infrared technology, on radar waves, the ones that use chemicals to get activated, and also there are the ones that use sound and acoustics to start working. Besides these, there are biosensors as well! In a nutshell, from infrared technology to energy beams and from chemicals to photo-elasticity – sensors use different mechanisms to work. They transmit data through a communication gateway, which could be any of the ones mentioned above, to enable us to get our work done in an effortless manner [4]. This could be for security, medical, or simply for entertainment. Sensors are surely the next tech-boom to conquer the world. It isn't so easy to determine their power and reach, if only sensors could read human emotion maybe we can start expecting something happening in this area too.

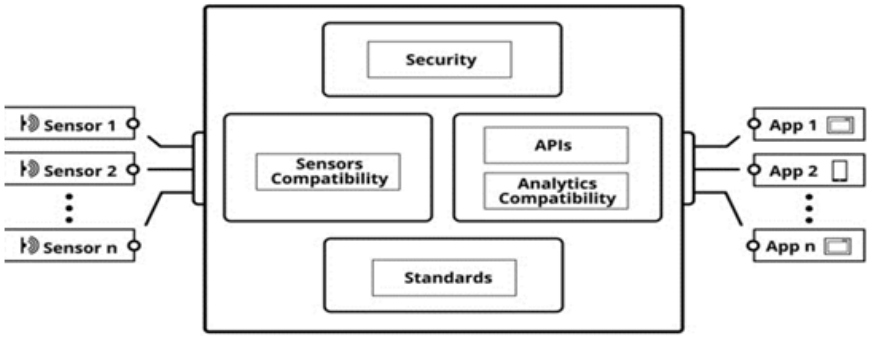

Fig 1: IOT Platform

The different sensors shown in **Figure 1** play an important role for the development of Internet of things applications along with security at each layer of architecture combined with physical security to add intelligence to the operation via data correlation and analytics. Without a standards-based security framework it is very difficult to create communication channels that are both secure and interoperable. An interoperable security solution is very important in order to prevent vendor lock-in and to enable the system to be extended if required. The Analytics compatibility which gives support for structured and non-structured data, ease of integration with existing operation, automation and control systems, the ability to operate in a distributed computing environment and API's for Integration of services, processes and systems in SOA application development paradigms. The different sensors which are used will vary as per the application and situation used.

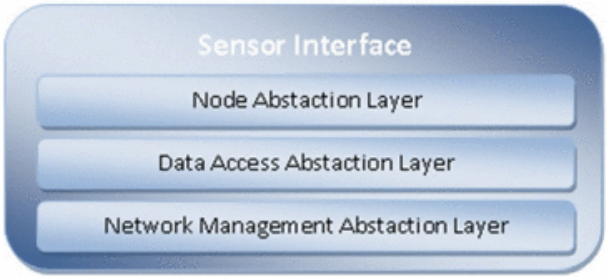

Fig 2: Information Model

The information model shown in **Figure 2** defines a conceptual model for representing data and describing the sensors and the commands accepted by the network. The context (Sensors, actuators and physical phenomena) is modeled by

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

means of an ontology based on the ontology Web Language (OWL), so that it is always possible to maintain an updated representation of the environment.

Abstraction layer: It is a logic layer between the building SAN Agent and the Base Statin. The Main goal of this component is to allow the separation of the physical networks from higher level components.This objective is achieved by defining an Abstract view and a uniform access interface to the different types of networks. A Data Centric communication allows application layers to be separated from issues related to network management and defining unique communication interface to higher levels makes each network independent from the peculiarities.

Node Abstraction layer: This layer allows the nodes to present their characteristics and functionalities to the higher levels in order to provide a homogenous mechanism for the discovery of various sensors deployed. The Description of the Networks is based on SensorML which provides a standard model and an XML, encoding of the measurement process. In particular, some discovery models.

Data Access Abstraction Layer:It provides an interface to collect sensor network data and transmit to the upper levels.The following data delivery models can be provided: Continuous in which information is transmitted at regular time intervals. Event –Triggered where information is transmitted only when a particular event occurs and Query Triggered where information is transmitted on a request.

The Network management Abstraction Layer: It provides an interface towards the functionalities related to network management system.

II. SERVICE ORIENTED ARCHITECTURE

A **Service-Oriented Architecture** (**SOA**) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network. The principles of service-orientation are independent of any vendor, product or technology.
A service is a self-contained unit of functionality. It is a discretely invokable operation. However, in the Web Services Definition Language (WSDL), a service is an interface definition that may list several discrete services/operations. And elsewhere, the term service is used for a component that is encapsulated behind an interface. This widespread ambiguity is reflected in what follows.

Services can be combined to provide the functionality of a large software application. SOA makes it easier for software components on computers connected over a network to cooperate. Every computer can run any number of services, and each service is built in a way that ensures that the service can exchange information with any other service in the network without human interaction and without the need to make changes to the underlying program itself. [5]
Integrating diverse sources of information takes place at three levels. At the lowest level is the communication medium that allows the exchange of information and control actions. Given such an interconnection, the communicating participants must agree on how information is represented; this middle level is variously called the format, data model, or object model. Finally, for such information exchanges to be useful the participants must have a way to discover what behaviors other devices can perform, and how to cause them to take particular actions; this third level is called service discovery.

In Web services, each information source or computational element describes itself in a Web Services Description Language (WSDL) file. As illustrated in **Figure 3,** a requestor of the service first obtains its WSDL, either directly from the service, as in device discovery, or indirectly from a repository. The WSDL is a complete machine-readable description of the service, revealing how information is represented and what behaviors are provided. It allows the requestor to bind to the provider of the service and establish any necessary translations in a fully automated fashion. Data sharing and behavior invocation are then conducted efficiently through the established service interface. XML and WSDL provide an automated framework for defining objects and operations. The application domain determines the specific objects and operations included in the services.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

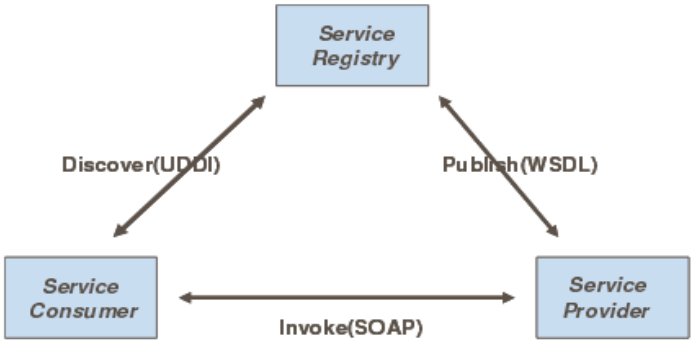

Fig 3: Implementation of SOA

In a typical SOA Composite application, we have collection of processes, services, data services with each layer building on top of the other to enable loosely coupled integration. Data services expose application interfaces as services which could in turn be orchestrated together to develop an application.

IV. SENSORS AS SERVICE IN IOT

In the Above, We have discussed how Sensors have become so much Importance in developing IOT devices and Service Oriented Architecture. Now the next generation of IOT devices is that they communicate themselves to be able to sense , perceive and react with minimal Human Intervention. To do so, Regardless of Different Networks these devices have to Communicate with Each other. It is necessary that The Ambience Intelligent Systems combine different networks in order to gather different types of Information .However, Each network has its own centralized management Systems. So, a number of Issues may arise, like duplication of Infrastructures, difficulties in expanding the existing systems or integrating the Sensor networks in to Elaboration systems [5].

A Possible Solution is to Combine Both Networks and Integration of Services i.e through Service Oriented Architecture. When developing software for the embedded domain, we also have to deal with hardware interaction like reading a sensor or writing data. SOAs which are often based on a ad-hoc request-response message pattern, control applications are typically event/data driven: the data is acquired by sensors and published to all connected services. These connected services can be actuator services triggering a hardware action or control services which can produce new output data based on their inputsOne of the most well established development and deployment of applications is through Service Oriented Architecture. It would be Interesting if Service orientation and sensors as a Service are combined together to Communicate devices. The SOA Approach is Asynchronous and allows heterogeneous Sensor Networks to communicate without time and location restrictions. Today, most sensors are small chips or circuit elements connected directly to powerful but inexpensive microcontrollers with sophisticated communication links (CMOS radios or wired interfaces)[6]. With intelligence and communication connected to every device, it should be easy to integrate them into rich networks.

V. SECURITY ISSUES

The Internet of things are everywhere around us. The TV when converted to a computer and connected to Internet or fridge when connected to a screen or when you install smart meter in house to save energy .People blindly follow all the instructions given by the Company. This smartness in every gadget has made life easy which is all good. The Question is where the data is stored .What are my privacy levels. Is any hacker in to the Household Private Data? Where Authenticity is Provided to these IOT Devices .Is The private Information going in to wrong hands. This is an Example of a Single House what if the same IOT devices are all deployed in global cites.

Concerns have been raised that the Internet of Things is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary. According to the Intelligence Survey conducted in the last quarter of 2014, 39% of the respondents said that security is the biggest

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

concern in adopting Internet of Things technology. In particular, as the Internet of Things spreads widely, cyber attacks are likely to become an increasingly physical (rather than simply virtual) threat. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and truck releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the onboard network. In some cases, vehicle computer systems are internet-connected, allowing them to be exploited remotely.

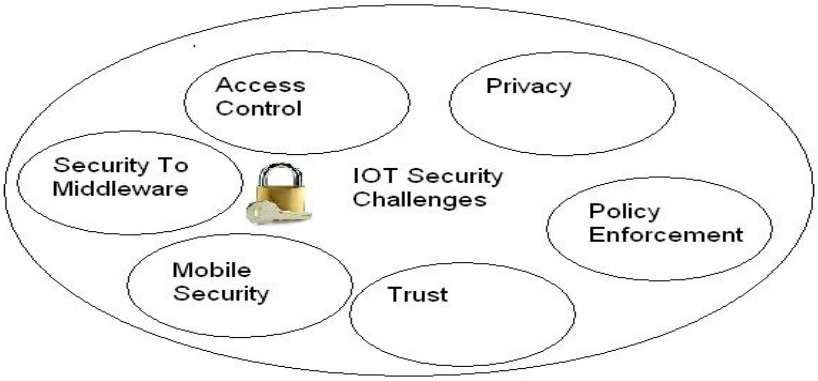

Fig 4: IOT Security Challenges

In traditional point to point architectures, data moves from point A to point B, is processed at point B, and the results are returned to point A. Thus, a secured connection between the two end points is adequate to ensure the integrity, confidentiality, and availability of the data. In an SOA environment, data originating at point A may travel through multiple intermediate points before arriving at the ultimate recipient. The subject identity must be provided, and the confidentiality and integrity of the data (in whole or as parts) must be protected and guaranteed from the point of origin to the destination.SOA, therefore, requires additional security components, as well as the adoption of new standards and specifications.

Extensive leverage of Open networks like internet, public cloud, Sensors, Web application. USB , Wireless, Bluetooth, Zigbee, GSM, etc and Unidentified, unauthorized and invalidated devices, Unauthorized remote access, Sensitive data exposure, Extensive dependence on software and applications have lead to security Issues like Access Control, Privacy, Policy Enforcement, Trust, Mobile Security and Security in Middleware in IOT devises that are shown in the above **Figure 4**.

IoT architecture modeled in a layered format is shown in **Figure5**. The Device layer at the bottom is the main source of data. It includes sensing/edge devices which sense the surrounding environment and transmit data in regular intervals. These sensors, in turn, may interact with an intelligent gateway. Gateway provides data aggregator and in few cases device level data processing capabilities. Data is funneled through a communication service provider network. CSP could either play the role of the network provider or it could move up the value chain to offer IoT infrastructure services. This layer would enable seamless connectivity with different M2M devices (data services in SOA) and offer the ability to remotely monitor and manage them for device connectivity.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

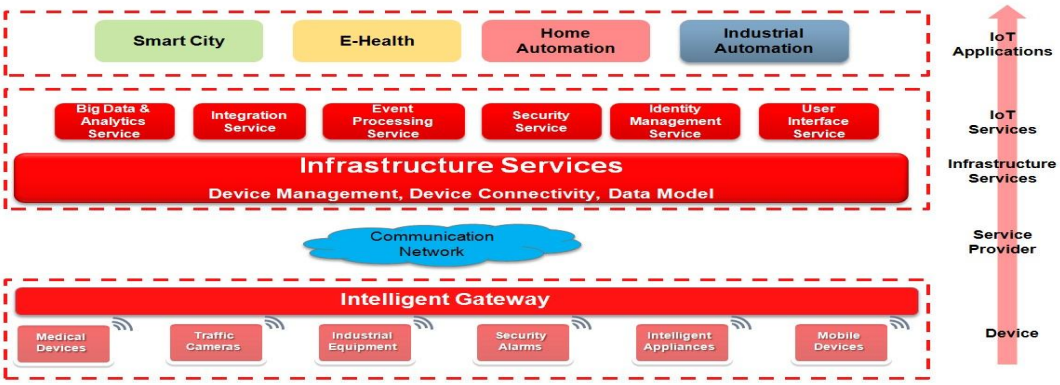

Fig 5: Layered IoT Architecture

IOT services layer is completed agnostic of underlying devices, communication protocols and connectivity semantics. This layer would include core set of services to build IoT applications:

a) Analyze data at real-time (event processing)
b) Act on M2M data & events (integration of service)
c) Enable historical, real-time and predictive analytics (Analytics Services)
d) Visualize operational and analytical data through mobile/desktop (UI Services)
e) Manage data security & identity of devices/apps (Security & Identity Management Service)

IOT platform enables this service oriented approach to build IOT applications. One of the most important features of SOA networking is the consolidation of privacy and security services such as authentication, authorization, firewalls, anti-malware programs and encryption. Such consolidation reduces the complexity of network administration, minimizes the risk of vulnerabilities and lowers operational costs. It can allow for a more robust and reliable network than would otherwise be possible. SOA networking also facilitates streamlined testing for compliance with standards and regulations. Therefore, breaches become less likely and can be corrected in the shortest possible time when they do occur.
An SOA network functions in three layers:

- The application layer includes all the software used by businesses and subscribers.
- The interactive services layer ensures constant and reliable communication among all users, devices and applications.
- The systems layer maintains the physical integrity of the network and ensures hardware interconnectivity and compatibility.

VI. SOA NETWORK SECURITY IN IOT

1. **Security at Message Level**: To establish security in the message the sender sends for the main receiver through the use of the interface, the security at the message level method is used. In this method, the different parts of a message are protected separately so that the message is only usable to intended sections located along the path

2. **Security as Service**: A security service can provide application programs with security capabilities (credit validation, authority validation, cryptography, etc.). This will not destroy the security sections in other services. The security service works fundamentally, and even indirectly. The security system is separated from the commercial logic(commercial services) in discussions on growth and development, because the security service is centralized and unrelated to applications; therefore, it is assigned to people who work as security personnel.

3. **Policy Oriented Security**: Security requirements and mechanisms should not be attached to the application program, but should be separately declared (mostly manually) as the “security policy”. The security logic is separated

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

from the commercial logic and is placed at the hands of security specialists. The instruction capability is also increased; and in the W-S-Security Policy standard, this logic is employed.

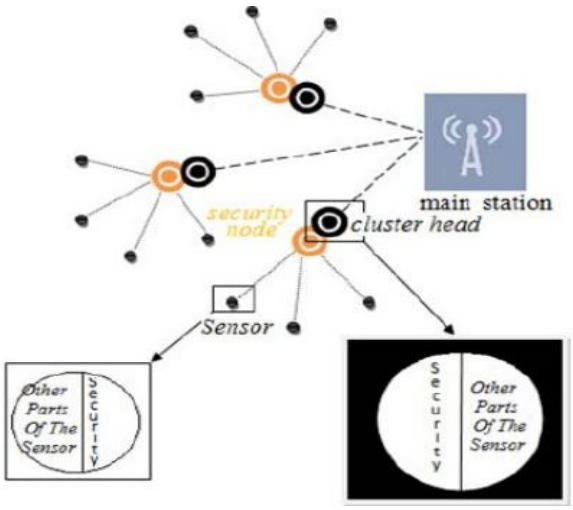

Fig 6: Security through the use of SOA

Since loose connections are used in SOA, there is slight dependence among components; and by taking advantage of this capability in wireless sensor networks, when one node is attacked the other nodes can continue their work. Moreover, by using SOA and the security as a service method, centralization in network security system becomes possible, as shown in the model in **figure 6**. A node is created next to the cluster head. This node, through interaction with the cluster head and the sensors, acts as an interface among the security sections of the cluster and the sensors and is of the cluster head type with a power source, a processor, etc.

The security node has capabilities including the following:

1. Recognizes the identity of the sensors so that by using SOA and the security at message level method, the information related to one specific node is not usable by other nodes and is only used by the intended nod. Therefore, if an enemy penetrates a node, it cannot have access to infinite information and information accessible to it will be limited.

2. Hides the information of other sensors so that this information is kept secret

3. Sends messages in the text mode

4. Reduces the volume of processed information in the sensor nodes; and because power is conserved, the life-time of the network is increased

As can be seen from the above model, this method does not cause any loss of the security of the sensors or other parts, but these parts carry on with their duties as before. Due to the interaction of the network with the Policy-oriented security method, the security logic is separated from the system logic; and this will cause improvement in the following capabilities [8]:

1. Capability to Interact More.
2. Capability to manage more connections.
3. Ease of Extension.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

VII. CONCLUSION AND FUTURE WORK

The IoT with Sensors presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces –such as the home, the car, and with wearable's and ingestible, even the body –poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. This Privacy can be improved through Service Oriented Architecture using sensors as service. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation.

REFERENCES

1. Bradley Mitchell , "Introduction to the Internet of Things (IoT)".
2. Feng Wang, Liang Hu, Jin Zhou, and Kuo Zhao "A Data Processing Middleware Based on SOA for the Internet of Things" Hindawi Publishing Corporation, Journal of Sensors, Volume 2015, Article ID 827045, 8 pages, http://dx.doi.org/10.1155/2015/827045.
3. Kaivan Karimi "The Role of Sensor Fusion in the Internet of Things".
4. Advances onto the Internet of Things: How Ontologies Make the Internet of Things Meaningful
5. https://en.wikipedia.org/wiki/Service-oriented_architecture
6. L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010. View at Publisher · View at Google Scholar · View at Scopus
7. L. Xu, W. He, and S. Li, "Internet of things in industries: a survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014. View at Google Scholar
8. Australian Journal of Basic and Applied Sciences, Security in Wireless Sensor Networks Based On Service-Oriented Architecture , Mohammad Ali Shamalizadeh, Shahaboddin Shamshirb and, Mohsen Amiri,Samiria Kalantari

BIOGRAPHY

T.V.Lakshmi Sukrutha is an Assistant Professor in Computer Science Engineering Department, Methodist College Of Engineering and Technology, Hyderabad, Telangana, India. She has received Masters Degree in Computer Science Engineering in 2012 from Jawaharlal Nehru Technological University, Hyderabad, Telangana, India. Her research interests are Web Programming Services, Service Oriented Architecture, Principles of Programming Languages, Cloud Computing, and Computer Organization.

S.Sri Lakshmi Anusha is an Assistant Professor in Computer Science Engineering Department, Methodist College Of Engineering and Technology, Hyderabad, Telangana, India. She has received Masters Degree in Computer Science Engineering in 2011 from Jawaharlal Nehru Technological University, Hyderabad, Telangana, India. Her research interests are Design Analysis and Algorithms, Web Programming, Cloud Computing.