International Journal of Advances in Engineering & Scientific Research, Vol.4, Issue 3, May-2017, pp 36-43 ISSN: 2349 –3607 (Online) , ISSN: 2349 –4824 (Print)

www.arseam.com
Impact Factor: 2.48

Cite this paper as : Shyna K and Vishal M (2017). "A Systematic Literature Survey: Internet of Things", International Journal of Advances in Engineering & Scientific Research, Volume 4,(Issue 3, May-2017), pp 36-43.

A SYSTEMATIC LITERATURE SURVEY: INTERNET OF THINGS

Shyna Kakkar
Assistant Professor
Department of Computer Science,
Dev Samaj College for Women,
Ferozepur, Punjab, India

Vishal Monga
Assistant Professor
Department of Management,
Ferozepur Institute of Management,
Ferozeshah, Punjab, India

Abstract:
IoT has given a novel form of communication called Machine-to-Machine communication which has quite promising future in India. According to WATconsult report, IoT will impact all the businesses in India by 2020. The Growth of IoT is due to the adoption of the internet, smart phones and social networks by humans. Agriculture and Healthcare are the major sectors where IoT can play a vital role for change and better quality of service. IoT suffers from many challenges in India like lack of consumer awareness, poor high speed data and high manufacturing cost. Internet of things has the ability to transform real world objects into smart objects. The main aim of this systematic study is to provide an overview of Internet of Things, its applications, security, architecture, and vital technologies for future research in the area of Internet of Things

Keywords- IoT, Cloud computing, Fog computing, Sensor

I. INTRODUCTION

'Internet of Things' term was first coined by Kevin Ashton in 1999 in the context of supply chain management [18]. The Word 'Thing' in the Internet of Things can be a person with a pulse monitor IoT device, an animal with a biochip transponder, a vehicle with sensors or any other object that can be assigned an IP address and provided with the ability to transfer data over a network. Internet of things (IoT) can be defined as the network of physical objects. IoT involves people to people, people to machine/things, machine to machine communication. It is estimated that there are 9 billion interconnected devices and it is expected to reach 24 billion devices by 2020.

The first internet appliance was a Coke machine at Carnegie Melon University in the early 1980s. Countries are adopting IoT in various fields such as retail, consumer wearable's, commerce and smart infrastructure. India's aim is for 20 percent market share in the next 5 years in IoT. 'Digital India' initiative highlights the key role of IoT and cloud technologies to usher in a digital revolution for growth in India. In the 2016-17 Union Budget, the government has allocated Rs. 7296 crores to its smart city mission which aims to build 100 Smart Cities. The success of this mission lies in the use of IoT, sensors, smart devices, connectivity, cloud and Big Data technologies.

IoT market in India is expected to grow to $15 billion by 2020 by adoption across sectors like transportation manufacturing, automotive and logistics, supply chain management, retail etc. In India, Telecom sector generates the highest revenue (36%) for IoT industry. Growing

adoption of cloud in IoT services and shifting focus over industrial IoT (IoT), rising market of machine-to-machine (M2M) communication, increasing trend of wearable technology applications are among the major factors driving IoT market in India. Enabling technologies of IoT are cloud computing, wireless sensor networks and Big Data.

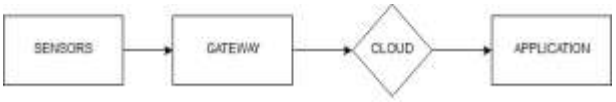

Fig1. Internet of Things (IoT)

II. LITERATURE REVIEW

The paper [1] proposed an intelligent door system using Internet of Things, which detects and send the email notification to the owner about the intrusion. It logs all the intrusion data into google spreadsheet of owner's google drive account. ADXL345 accelerometer detects the change in motion of the door. Raspberry pi has been used to read sensor data. Sensor data is sent to the Amazon Web Services Internet of Things (AWSIoT) console.AWS Simple Notification Service (SNS) will send out email notification to the concerned owner based on the AWS IoT console message based on the messages from the AWS IoT console. All the intrusion logs are also stored in google spreadsheet by OAuth2.0 protocol to access related google Application program interface (APIs).The proposed system can be used as a prototype in strengthening door security in many applications such as bank burglary, home invasions, Ram-raiding, office door breaching and lock picking.

The paper [2] proposed IoT based attendance system. Attendance system is designed with the use of micro controller ESP8266 12e and OLED display. OLED display shows the names of the students whose fingerprint is scanned. A fingerprint module R305 has been used to scan and recognize the fingerprints. Other components used are wires, switches, and PCB. The system has a transmitting module to send the fingerprint matched ID.A server in attendance system receives fingerprint matched ID from the transmitting module. After processing the data, student attendance is calculated in percentage. A student can check their attendance through the android application provided by the system.
This application facility sends push notifications when assignments are issued by teachers or the attendance of particular student is low. The System can be used for security purposes where high-level security is desired.

The paper [3] proposed IoT based Intelligent Safety & Location Tracking Device for Old Age & Women. The purpose of the system is to assist parents to locate missing or lost women and children. It works using GPS and SMS and detects the child location. The System sends the location to parents using GPRS module. An application is helpful for parents that will allow them to send a location request to a child side then retrieve the location from the request reply and point it on a map. Another application is also provided for child side that gathers the necessary information of the smart phone that will be used to locate the smart phone. In the case of extreme emergency, An SOS button is available in the system which sends the location of the device to registered mobile for help from parents or person. The System is comparatively low-cost solution and performance of the device is accurate and reliable. The web version is used to see current the location and send updated location to server. This system use ARM-LPC2138 as microcontroller and for GPS S1216R module has been used. The server has been created using filezilla tool. One server collects the data from the system and sends it through GPRS.

The paper [4] proposed a medical alert system for remote health monitoring using sensors and cloud. It uses heart rate sensors and temperature sensors for physiological monitoring. Accelerometer sensors can be attached to human arm to determine patients' movements and 3D cameras can be used for visual monitoring of elderly patients. Sensor nodes send signals and received signal is sent to an android application where the received values are checked against threshold values. When an anomaly is detected, the application generates an alert to the doctors and caretakers via a Personal Data Assistant (PDA) or cell. All the sensed values are sent to the Cloud server where the data is stored for long-term analysis and interpretation by the doctor. The Hardware part consists of Temperature sensor (LM35), Heart beat sensor and Eye blink sensor, Power supply unit, GSM unit (SIM 300), 8051 development board, P89V51RD2 IC, LCD and ADC card (0809) and PhilipsP89V51RD2 microcontroller. Future enhancements possible are to increase Cloud security as the data being stored is Sensitive health-related data. Security mechanisms such as authorization, authentication and user access control should be incorporated in the system.

The paper [5] proposed smart farming water holding the capacity of the particular patch programmed on the already installed automatic irrigation system. If the value goes below that threshold level, then its respective water pipe will get ON and the water level in that patch of field will increase the chemical sprinkler for different crops on patch can be programmed and its timer can also be set as per needed, so not to lose the sustainability of the farm. A GSM+ARDUINO combination has been used to receive information of the farm on the mobile device by just texting the pre programmed format of message to the sim card used in GSM module. Information uploaded on an open source platform called THINGSPEAK. Different crops can be cultivated on a single field divided in the form of patches, by just installing this automatic plant irrigation system (consisting of soil sensors, water level indicators and chemical sprinkler) according to the requirements of the crops. In automated water control system, and BC147 is used an amplifier and ARDUINO is being used as a microcontroller. Further enhancement of this system can be an Intruder alarm or buzzer can be used so that any human/animal intruder cannot disrupt the productivity of the farm. A camera can be installed to monitor the live farm in real time system. A study based on the removal of excess rain water can be implemented as well.

The paper [6] proposed smart pollution detection and tracking system. The Pollution from the vehicle is sensed using the MQ7 Arduino which is connected to the Arduino board which in turn is connected to the GPS module. The Amazon AWS IoT is connected to Arduino board using MQTT connection. This enables a secure connection with the Arduino .The data that is received is checked against the threshold value. If the value exceeds the threshold value then notification is sent to the users mobile phone.MQ7 Gas sensor is preferred to be the cheapest and it can be coded with an Arduino board which enables easy implementation.

III. IOT APPLICATIONS

1) Smart cities: A smart city is an urban development vision to integrate information and communication technology (ICT) .IoT can be used to monitor parking areas for availability. It can also be used for measurement of energy radiated by wifi routers and cell stations. IoT can be used for building, bridges and historical monuments to check its material condition.

2) Security & Emergencies: IoT can be used to detect the presence of liquid in sensitive buildings. IoT also helps to detect explosive and harmful gases.

3) Smart agriculture: IoT application in agriculture is to monitor moisture of soil and also used to keep a check on crop health. It can be used to automate the process of fertilizers usage based on weather conditions.

4) Domestic & Home Automation: IoT can be used to remotely monitor and manage our home appliances and cut down monthly bills and resource usage. IoT application is also in Intrusion Detection Systems to detect windows and doors openings to prevent intruders.

5) Health Care: IoT devices are used to assist elderly or disabled people living alone. It also helps to monitor and control conditions inside freezers storing medicines, vaccines. The Application also lies in the monitoring of patients conditions inside the hospitals and in old people's home.

6) Industrial Control: IoT is used to monitor oxygen levels and toxic gas inside chemical plants for the safety of goods and workers. It can also be used to monitor ozone level during dry meat process in food factories.

IV. IEEE PROTOCOLS FOR IOT COMMUNICATION

IoT devices need wireless communication protocols to send sensor data to other devices. Various wireless technologies can be implemented in hardware for Machine to Machine (M2M) and the Internet of Things (IoT) communication such as Z-Wave, ZigBee, IrDA, Bluetooth Low Energy, Radio Frequency Identification (RFI), Bluetooth, Near, Wi-Fi etc. The Different application requires wireless technology according to its requirements like smart watch and fitness tracker needs short range and low energy network. Smart car requires high-speed network like 4G LTE. The Institute of Electrical and Electronics Engineers (IEEE) has set

the standards for common types of wireless technologies used for personal area networks. The 802.15 task groups include: WPAN/Bluetooth, Coexistence, Low Rate WPAN, High Rate WPAN, Body Area Networks, mesh Networking and Visible Light Communication.

1. *1) IEEE 802.15.4-Zigbee*
2. It is open global standard designed for IOT Machine-to-Machine communication. Zigbee does not require much power and is inexpensive. It offers 128-bit AES encryption and can also be used in mesh networks.
3. *2) IEEE 802.15.1: Bluetooth and BLE*

Bluetooth and Bluetooth Low Energy (BLE) are used to transfer data over short distances. Bluetooth Low Energy use less power compared to standard Bluetooth.BLE is used in smart devices such as smart watch and fitness watches etc.BLE was introduced by Nokia Company in 2006.It is supported by majority of operating systems and smart phones. Bluetooth uses UHF radio waves for data transfer.

4. *4) IEEE 802.11: WiFi*
5. Wifi uses radio waves (RF) for device communication. It is used to connect routers to computer and other devices. Wifi use the frequencies 2.4GHz UHF and 5GHz SHF ISM radio bands. 802.11b, 802.11g, and 802.11n run on the 2.4GHz ISM band.
6. *3) IEEE 802.16: WiMax*

WiMax stands for Worldwide Interoperability for Microwave Access. It allows data transfer at a rate of 30–40 megabits per second.
Some other communication protocols for IOT are following:

-Advanced Message Queuing Protocol
-Message Queuing Telemetry Transport (MQTT)
-Very Simple Control Protocol (VSCP)
-Constrained Application Protocol (CoAP)
-Extensible Messaging and Presence Protocol (XMPP)

V. IOT ARCHITECTURE

Different architectures have been proposed by different researchers, According to International telecommunication Union, IoT architecture has 5 layers.
1) Sensing layer
2) Access layer
3) Network layer
4) Middleware layer
5) Application layer

VI. IOT COMMUNICATION MODELS

In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452), which outlines a framework of four common communication models used by IoT devices.

-Device-to-Device Communications Model

-Device-to-Cloud Communications Model

-Device-to-Cloud Communications Model

-Device-to-Gateway Model

VII. IOT AND FOG COMPUTING

Cloud computing fits all the IoT based applications. Some problems are still unsolved since IoT applications usually require mobility support, location-awareness, geo-distribution and low latency .Fog computing technology can also be used for Internet of Things .Fog Computing extends the Cloud Computing paradigm to the edge of the network. Fog computing is a distributed computing model that fetches centralized located data storage, processing and application given to the network edge [15]. Fog computing is not replacement of the Cloud Computing. Data collected by sensors are not sent to the cloud server for processing instead it is sent to devices like the access point, routers for processing. Fog computing provides benefits of reduced latency and improved Quality of service. Some Data is processed locally and responses are sent back to the end users without the use of the cloud.
Fog computing is typically used in applications where

time is critical and requires an immediate response like in medical healthcare IoT system where a delay in sending of data at cloud and processing may be pernicious for the ill patient. Another example where fog computing can be used is in smart vehicle where the sudden accidental situation requires quick decision to be taken by the smart vehicle system to avoid accident. In such cases, fog nodes can collect the data from sensor and process it at the edge of network and decision is send back in the fraction of seconds to a smart device. Only crucial data now can be transferred to cloud for storage and analysis.

TABLE I
DIFFERENCE BETWEEN CLOUD AND FOG COMPUTING

Attribute	Cloud Computing	Fog computing
Latency	high	low
Attack on data	High chances	Low chances
Location of server nodes	Within the internet	At the edge of the local network
Real time interactions	Supported	Supported

VIII. METHODLOGY FOR TIME CRITICAL IOT APPLICATIONS USING FOG COMPUTING

Step 1.Different sensors and actuators are used to capture information. Sensors can be Temperature sensors, Chemical sensors, Light sensors and Humidity sensors etc. Small sensors can be embedded in smart phones and wearable.

Step 2.Data collected from the wireless sensor network is passed to the internet gateway. Data acquisition systems (DAS) perform data aggregation and conversion functions. The Internet gateway receives the aggregated and digitized data and routes it over Wi-Fi, wired LANs, or the Internet to fog node.

Step 3.Time critical IoT system requires an immediate decision. Preprocessing and analysis is performed at the edge of the networks at fog node. Device that has capability of computing, storage, and network connectivity can be a fog node. Sensitive data is analyzed on the fog node which is near to the things generating the data. Fog node use IoT enabled applications for real-time control and analytics, with millisecond response time. It also provides transient storage and then sends the data to the cloud using communication protocols.

Step 4. Data send by fog node that is less time sensitive is used for historical analysis, big data analytics, and long term storage. It receives and aggregates data summaries from many fog nodes.

IX. IOT OPERATING SYSTEMS

IoT operating system for IoT system development should be based on the application level, API requirements and hardware requirements. Some of IoT Operating Systems are Alljoyn, Raspbian, RIOT, Contiki and Spark etc. RIOT OS, LiteOS and Tiny OS are an operating system for Internet of Things (IoT) devices.

TABLE II
FEATURES OF IOT OPERATING SYSTEMS

Operating System	Minimum Memory	Language Support	Multithreading
RIoT OS	1.5KB	C/C++	YES
LiteOS	4KB	C	YES
Contiki	2KB	C	YES
TinyOS	1KB	nesC	Partial

X. IOT SECURITY

Resolving Security issues in IoT is a big challenge and should be considered in every aspect of IoT system. Security should be provided in the physical device itself, the way device connects, data is stored, during cloud processing and, or at the user-interface. Reasons for security concerns are:

a) IoT devices operate without human intervention which makes unchallenging for the attacker to physically gain access to them.
b) IoT devices communicate using wireless networks so

there is a threat to user's confidential data.
c) Some IoT devices might not support complex security schemes due to low power and computing resource capabilities.

A. Data Encryption

Internet of things applications collects tons of data. Data privacy is a concern of device user. Data can be protected through encryption. Secure Sockets Layer protocol or SSL can be used to protect data present online. Data should also be encrypted during transfer to cloud or device. Wireless protocol with in-built encryption is the solution for protection of sensitive data.

B. Data Authentication

There should be a way to authenticate data communicated in IoT device. For instance, without authentication, one can send fake data to your sensor node to manipulate. Authentication issues may not cause that serious damage but they definitely pose a security risk. Solutions to avoid such risks are to use simple static password, two-factor authentication, biometrics and digital certificates.

C. Network security

The network which connects the IoT devices should be protected and secured to back-end systems on the internet. IoT network security is more challenging than traditional network security because there is a wide range of standards, communication protocols and device capabilities all can cause major issues and increased complexity. Solutions to protect the network include traditional security features such as antivirus and antimalware and other features like firewalls and intrusion prevention and detection systems. Sample vendors of these are Cisco, Senrio, Bayshore Networks and Darktrace

D. IoT API Security

It provides the ability to authenticate and authorize data transfer between applications IoT devices and back-end systems using documented REST-based APIs. API security is important for protecting the integrity of data transferred between back-end systems and edge devices. It ensures that only authorized apps, devices and developers are communicating with APIs as well as detecting potential threats and attacks against specific APIs.

XI. IOT SECURITY ATTACKS

Gartner, Inc. forecasts that 8.4 billion connected things will be in use worldwide in 2017, up to 31 percent from 2016, and will reach 20.4 billion by 2020 [7]. It is estimated that total spending on services and endpoints will reach almost $2 trillion in 2017. All the connected devices whether it is a smart refrigerator or smart fitness tracker are part of networks now. Besides their benefits to the users they also pose an increasing security and privacy risk.

A. Physical attacks

Physical attack vandalizes hardware components. IoT devices operate in the outer environment where they are exposed to physical attack. It is due to unattended and distributed nature of IoT.

B. Botnets

A botnet is a network of systems designed with the purpose of remotely taking control and distributing malware. Recently a new bot named Persirai the has a infected 1,000 different IP camera models and was discovered by Trend Micro

C. Denial-of-service (DoS)

DoS attack is an attempt to make a machine or network resource unavailable to its intended users [18]. DoS do not usually try to steal information or leads to security loss. In October 2016, the largest DDoS attack was launched on service provider Dyn using an IoT botnet. Major companies suffered from this attack at that time which includes Netflix Twitter, the Guardian, Reddit, and CNN.

D. Destructive attacks

IoT devices exposed to security issues can be exploited by cyber criminals to create large-scale disruption and destruction of life and property. Examples are revenge attacks and terror attacks.

E. Attack to privacy

Password-based attacks are used for the intrusion. There are two different methods of password based attack:

1) Brute force attack: It uses cracking tools to try all possible combinations of passwords to uncover valid passwords.

2) Dictionary based attack: In this attack, all type of password combinations are tried to guess user password.

According to the finding of Study on Mobile and Internet of Things Application Security by Ponemon Institute sponsored by IBM and Arxan Technology that most organizations are concerned about an attack against IoT apps used in the workplace. Respondents for the study were more concerned about hacked through an IoT app (58 percent) than a mobile app (53 percent) [20].

XII. CONCLUSION

IoT has potential to bring the industrial revolution crucial to businesses government and consumers, transforming all sectors including automation, agriculture, manufacturing automotive, energy, consumer electronics and utilities, home automation healthcare, infrastructure, etc. IoT has potential to create a big impact in the near future. IoT generates a lot of data which demands focus on cryptographic data storage and the use of edge computing, sophisticated analytics and Artificial intelligence. Research scope for IoT includes the need of self-powering sensors, self - configurable and self-healing software algorithms and IoT complex data analysis.

REFERENCES

[1] S. Nazeem Bash, Dr. S.A.K. Jilan, Mr. S. Arun, "*An Intelligent Door System using Raspberry Pi and Amazon Web Services IoT*", Vol. 33, Number 2, March 2016, IJETT

[2] Anilkumar Patil, Akash Mahla, Sonica Sonawane, *"IoT based attendance system*", Vol. 04, Issue 02, Feb 2017, ,IRJET

[3] Prof. Nitin S. Wagh, Prof. Ravindra, P. Shekikar, "*Intelligent Safety & Location Tracking Device for Old Age & Women Using Concept of "Internet of Things"*, Vol. 5, Issue 10, October 2016, IJIRSET

[4] Indumathy N, Dr. Kiran Kumari Patil, "*Medical alert system for remote health monitoring using sensors and cloud computing*", Vol. 04 ,Issue 02 , Feb 2017, , IJRET

[5] Hariharr C Punjabi, Sanket Agarwal, Vivek Khithani, Venkatesh Muddaliar, Mrugendra Vasma, "*Smart farming using IoT*", Vol. 8, Issue 1, January - February 2017, pp. 58–66, IJECET

[6]Marina Sruthi. M, Dr. L. Josephine Mary, "*Smart Pollution Detection and Tracking System Embedded With AWS IOT Cloud",* Vol. 6, Issue 4, April 2016, IJARCSSE

[7] http://www.gartner.com/newsroom/id/359891

[8] Mohamed Abomhara, Geir M. Køien, "*Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks*", Vol. 4, 65–88, 22 May 2015, Journal of Cyber Security

[9]6-in-demand-internet-of-things-iot-security technologies, retrieved July 23, 2017, from http://jikeme.com

[10]http://www.cisco.com/c/dam/en_us/solutions/trends /IoT/docs/computing-overview.pdf

[11]Anish Vahora, Siddharaj Gogre, Palash Gandhi, Pratik Vaswani, "*Comprehensive study of Smart Parking System*", Volume 6, Issue 1, January - February 2017, IJTTCS

[12]Reshma Shinde, Ritika Pardeshi, Archana Vishwakarma, Nayan Barhate, "*Need for Wireless Fire Detection Systems using IOT*", Vol. 04, Issue 01, Jan - 2017, IRJET

[13] Uday Dodla, "*How the Internet of Things Is Digitizing Agriculture & Speeding up Rural Development*", http://www.indiatimes.com July 26, 2017

[14] Nandavarapu Kiran**, "***Transformation of B2B Business by IoT in India*", July 27, 2017, DQINDIA online

[15] Nisha Peter, "*FOG Computing and Its Real Time Applications*", Volume 5, Issue 6, June 2015, International Journal of Emerging Technology and Advanced Engineering

[16] Nupur Tyagi, "*An overview on IoT enabling technologies"*, Volume X, Issue I, Jan 16, International Journal of Computer Engineering and Applications

[17] http://www.cisco.com

[18] https://kb.cyberoam.com

[19] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, "*Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions"*

[20] 2017 Study on Mobile and IoT Application Security, Retrieved July 21, 2017, from https://www.arxan.com