IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Internet of things: A Survey on Architecture, Applications, Security, Enabling Technologies, Advantages & Disadvantages

Farheen Fatima[1], Batul Naeem Husain[2], Mohammed Azharuddin[3], Mohammed Abdul Mabood[4]

Computer Science Department, MuffakhamJah College of Engineering & Technology, Hyderabad[1, 2, 3, 4]

Abstract: Internet of Things (IoT) is the emerging trend in the field of Technology. This technology has the potential to revolutionize the way of living in future. It represents the first true evolution of internet. Internet of Things (IoT) aims to connect intelligent communicating 'things', which are assigned an IP address, to internet and makes one thing to communicate with other thereby providing remote sensing and control. IoT devices are ubiquitous, context-aware and enable ambient intelligence .It opens door to endless opportunities which might have great impact on our lives. This article reports on the current state of research on the Internet of Things by examining the architecture, applications, security, technologies, advantages and disadvantages of Internet of Things (IoT).

Keywords: Internet of Things, RFID, Microsoft Azure, Zigbee, Cloud computing.

I. INTRODUCTION

Introduction means something that existed before IoT, history before IoT came into existence and once that is over, then keep the remaining part as it is.

The concept of the IoT comes from Massachusetts Institute of Technology (MIT)'s Auto-ID centre in 1999. The MIT Auto-ID Laboratory created the IoT using Radio Frequency Identification (RFID) and Wireless Sensor Networks.

IoT is a foundation for connecting things, sensors, actuators, and other smart technologies, thus enabling person-to-object and object-to-object communications. The term "Internet of Things" was coined by Kevin Ashton. IoT is defined as "device to device communication without any human interaction".

An author defined IoT in the form of equation as shown below. The early work on IoT was done using the concept of RFID(Radio Frequency Identification) and it was seen as prerequisite for Internet of Things. Internet of Things today is seen as convergence of many technologies such as embedded systems, wireless communication, internet, micro-electromechanical systems, cloud computing, data mining etc.

The words "Internet" and "Things" mean an inter-connected world-wide network based on sensory, communication, networking, and information processing technologies, which might be the new version of information and communications technology [1] (ICT). IoT is in its early stages of development. Sensor technology is playing a vital role in the advancement of IoT. The applications of IoT are carried in the areas of Media, Environmental monitoring, Infrastructure management, Manufacturing, Energy management, Medical and healthcare systems, Building and home automation, Transportation, Large scale deployments.

However, the application of the IoT is not only restricted to these areas.

A lot of research is being carried out by the professionals on IoT the major one is the work on smart cities. RFID techniques and related identification technologies will be the important feature of the upcoming IoT. Many countries today are making investment in IoT and the day by day IoT is progressing. In March 2015 the European Commission initiated the creation of the Alliance for Internet of Things Innovation [2] (AIOTI). IoT indicates that everything can be made to communicate and can be accessible.

Physical Objects
+
Controller,Sensor and Actuators
+
Internet
=
Internet of Things

Fig.1 Typical IoT Equation

II. LITERATURE SURVEY

The Internet of Things (IoT) is a network of physical objects that contain embedded technology to communicate and interact with their internal states or external environment.

To make something an Internet of Things device we need to give it senses and provide it some unique identity so that we can communicate with it from any part of the world [3].

A. Event Producers

Event Producers are Sensors that detect or measure a physical property and convert it into some kind of electronic representation.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

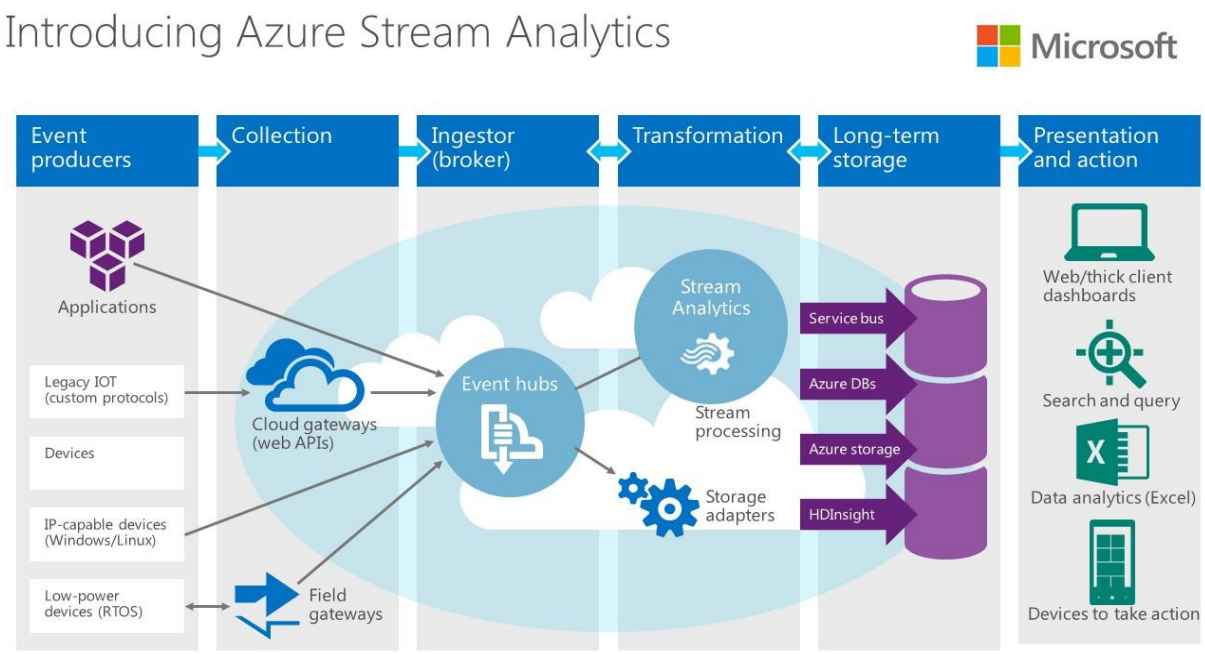

Fig. 2IoT Architecture

Sensors may be passive or active – with the difference being the amount of intelligence embedded in the sensor.
Sensors are sophisticated devices that are frequently used to detect and respond to electrical or optical signals .A Sensor converts the physical parameter (for example: temperature, blood pressure, humidity, speed, etc.) into a signal which can be measured electrically.
Device provides the intelligence needed to work meaningfully with the data provided by the attached Sensor(s). Here the data from the sensor is translated, transformed and possibly combined with other data, this processing transforms the data from simple bits and bytes to useful information. Some important devices are Arduino, Raspberry pi-2, IntelGalileo, Intel Edison, Samsung ARTIK.

B. Collection
A cloud storage gateway provides basic protocol translation and simple connectivity to allow the incompatible technologies to communicate transparently.
The gateway may be a stand-alone computing device or a virtual machine image that provides basic protocol translation and connectivity that allows incompatible technologies to communicate transparently.
A field's gateway is simply an aggregation point for a range of in-place sensors. Many low powered / basic devices do not have enough capacity to run secured HTTP sessions so in these cases there will typically be a gateway to which these devices send their data. The gateway can aggregate / store and then forward the data securely onto Azure Event Hubs.

C. Event Hubs
Event Hub is a highly scalable publish-subscribe event ingestor that can intake millions of events per second so that you can process and analyze the massive amounts of data produced by your connected devices and applications. Once collected into Event Hubs you can transform and store data using any real-time analytics provider or with batching/storage adapters.

D. Transformation
Stream Analytics : Azure Stream Analytics service in the cloud lets you rapidly develop and deploy a low-cost analytics solution to uncover real-time insights from devices, sensors, infrastructure and applications and also real-time remote management and monitoring or gaining insights from devices like mobile phones and connected cars.
Storage Adapters: In computer hardware, a host controller, host adapter, or host bus adapter (HBA) connects a host system (the computer) to other network and storage devices.

E. Long-Term Storage
Azure Service Bus is a generic, cloud-based messaging system for connecting just about anything—applications, services and devices—wherever they are. Connect apps running on Azure, on-premises—or both. You can even use Service Bus to connect household appliances, sensors and other devices like tablets or phones to a central application or to each other.
Microsoft Azure SQL Database is a cloud-based service from Microsoft offering data-storage capabilities (similar to Amazon Relational Database Service) as a part of the Azure Services Platform. AzureSQL Database allows users to make relational queries against stored data, which can either be structured or semi-structured, or even unstructured documents.
Azure HDInsight deploys and provisions Apache Hadoop clusters in the cloud, providing a software framework designed to manage, analyze, and report on big data with high reliability and availability. HDInsight uses the Horton works Data Platform (HDP) Hadoop distribution.

F. Presentation and Action:

1) Client Dashboards: The Dashboard (located under the Overview tab) is the very first screen you see when you access a Client, a Project, a Folder or a Workspace. It provides you with the most recent and most urgent information from all modules.
2) Search and Queries: A web search query is a query that a user enters into a web search engine to satisfy his or her information needs. Submission of a query results in information retrieval.
3) Data Analytics with Excel: Excel is probably the most commonly used spreadsheet for PCs. It is easily used to do a variety of calculations, includes a collection of statistical functions, and a Data Analysis ToolPak. It is an electronic spreadsheet program used for storing, organizing and manipulating data. Excel uses formulas to perform mathematical calculations ranging from the simple to the very complex. The program can also be used for graphing data [4].

III. IOT APPLICATIONS

The Internet of Things (IoT) allows us to use technology to enhance our comfort, improve our energy efficiency and simplify the tasks that consume our home and work life and give us greater control over our lives.

Potential applications of the IoT are numerous and diverse, permeating into practically all areas of every-day life of individuals, enterprises, and society as a whole. The main Internet of Things applications, which span numerous applications domains, are smart energy, smart health, smart buildings, smart transport, smart industry and smart city [5].

From building and home automation to wearables, the IoT touches every face of our lives. It makes developing applications easier with hardware, software and support to get anything connected within the IoT.

The vision of a pervasive IoT requires the integration of the various domains into a single, unified, domain and addresses the enabling technologies needed for these domains while taking into account the elements that form the third dimension like security, privacy, trust, safety.

A. Smart Cities

In a few years, we will see the development of Mega city corridors and networked, integrated and branded cities. Urbanization as a trend will have diverging impacts and influences on future personal lives and mobility. Rapid expansion of city borders, driven by increase in population and infrastructure development, would force city borders to expand outward and engulf the surrounding cities to form mega cities, each with a population of more than 10 million.

This will lead to the evolution of smart cities with eight smart features, including Smart Economy, Smart Buildings, Smart Mobility, Smart Energy, Smart Information Communication and Technology, Smart Planning, Smart Citizen and Smart Governance.

The role of the city governments will be crucial for IoT deployment. Running of the day-to-day city operations and creation of city development strategies will drive the use of the IoT. Therefore, cities and their services represent an almost ideal platform for IoT research, taking into account city requirements and transferring them to solutions enabled by IoT technology.

B. Smart Energy and Smart Grid

There is increasing public awareness about the changing paradigm of our policy in energy supply, consumption and infrastructure. For several reasons our future energy supply should no longer be based on fossil resources or nuclear energy. In consequence future energy supply needs to be based largely on various renewable resources.

This supply demands an intelligent and flexible electrical grid which is able to react to power fluctuations by controlling electrical energy sources (generation, storage) and sinks (load, storage). Such functions will be based on networked intelligent devices (appliances, infrastructure, and consumer products) and grid infrastructure elements, largely based on IoT concepts.

Although this ideally requires insight into the instantaneous energy consumption of individual loads (e.g. devices, appliances or industrial equipment), information about energy usage on a per-customer level is a suitable first approach.

C. Smart Home

The rise of Wi-Fi's role in home automation has primarily come about due to the networked nature of deployed electronics where electronic devices (TVs and AV receivers, mobile devices, etc.) have started becoming part of the home IP network and due the increasing rate of adoption of mobile computing devices (smartphones, tablets, etc.).

A Connected Home can mean different things to different people, but it's essentially a home with one or more (or many) devices connected together in a way that allows the homeowner to control, customize and monitor their environment.

That can mean anything from a programmable learning thermostat to a security system of window, door and motion sensors, to the future of smart appliances. The common denominator is that ideally all of these devices should come together into a connected ecosystem that is easy for the homeowner to access and control. If the IoT is fundamentally about making our lives easier and more connected, then the implications for a truly Connected Home are game-changing.

D. Smart Health

The market for health monitoring devices is currently characterised by application-specific solutions that are mutually non-interoperable and are made up of diverse architectures.The IoT can be used in clinical care where hospitalized patients whose physiological status requires close attention can be constantly monitored using IoT-driven, non-invasive monitoring.

Wearable technology is a blanket term that covers a vast array of devices that monitor record and provide feedback on you or your environment. Broadly speaking, you can divide wearables along two lines:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

1) Fitness and Environment**:** Fitness bands and watches and even smart clothes are able to monitor and transmit data on your daily activity levels through step counting, heart rate and temperature.
2) Health**:** These wearables monitor crucial health factors like oxygen saturation, heart rate and more, and can communicate any results outside of a programmed range to the patient and to her physician.

E. Smart Mobility and Transport

The connection of vehicles to the Internet gives rise to a wealth of new possibilities and applications which bring new functionalities to the individuals and/or the making of transport easier and safer. IoT is an inherent part of the vehicle control and management system. Already today certain technical functions of the vehicles' on-board systems can be monitored on line by the service centre or garage to allow for preventative maintenance, remote diagnostics, instantaneous support and timely availability of spare parts. For this purpose data from on-board sensors are collected by a smart on-board unit and communicated via the Internet to the service centre.

IoT can be used for enabling traffic management and control. Cars should be able to organise themselves in order to avoid traffic jams and to optimise drive energy usage. This may be done in coordination and cooperation with the infrastructure of a smart city's traffic control and management system. Additionally dynamic road pricing and parking tax can be important elements of such a system. Further mutual communications between the vehicles and with the infrastructure enable new methods for considerably increasing traffic safety, thus contributing to the reduction in the number of traffic accidents.

F. Industrial Automation

The Internet of Things has profound implications for industrial automation and the industrial internet of things. With wireless connectivity, advanced sensor networks, machine-to-machine communications, traditional industrial automation will become more informed and more efficient than ever before.

The IoT will connect the factory to a whole new range of applications, which run around the production. This could range from connecting the factory to the smart grid, sharing the production facility as a service or allowing more agility and flexibility within the production systems themselves. In this sense, the production system could be considered one of the many Internets of Things (IoT), where a new ecosystem for smarter and more efficient production could be defined.

The IoT applications are addressing the societal needs and the advancements to enabling technologies such as Nano-electronics and cyber-physical systems continue to be challenged by a variety of technical (i.e., scientific and engineering), institutional, and economical issues.

IV. IOT SECURITY

IoT security is the area of endeavour concerned with safeguarding connected devices and networks in the Internet of things.

Although it has been with us in some form and under different names for many years, the Internet of Things (IoT) is suddenly everywhere. The Internet of things involves the ability to connect, communicate with, and remotely manage an incalculable number of networked, automated devices via the Internet and the ability to automatically transfer data over a network. It consists of devices other than computers, like household appliances, smart TVs and hardware components.

The main problem is that because the idea of networking devices is relatively new, security has not traditionally been considered in product design. Products are often sold with old operating systems and software. Furthermore, purchasers often fail to change the default passwords on devices; or if they do change them, fail to select sufficiently strong passwords.

A. The Evolution of Network Security

Protection of data has been an issue ever since the first two computers were connected to each other. With the commercialization of the Internet, security concerns expanded to cover personal privacy, financial transactions, and the threat of cyber theft. In IoT, security is inseparable from safety. Whether accidental or malicious, interference with the controls of a pacemaker, a car, or a nuclear reactor poses a threat to human life.

Security controls have evolved in parallel to network evolution, from the first packet-filtering firewalls to more sophisticated protocol and application aware firewalls.

These controls attempted to keep malicious activity off of corporate networks and detect them if they did gain access. If malware managed to breach a firewall, antivirus techniques based on signature matching and blacklisting would kick in to identify and remedy the problem.

Applying these same practices or variants of them in the IoT world requires substantial reengineering to address device constraints. Blacklisting, for example, requires too much disk space to be practical for IoT applications.

The endless variety of IoT applications poses an equally wide variety of security challenges. For example, in factory floor automation deeply embedded programmable logic controllers (PLCs) that operate robotic systems are integrated with the enterprise IT infrastructure. How can those PLCs be shielded from human interference while at the same time protecting the IT infrastructure and controlling the security controls available?

B. Building Security from the Bottom Up

Security is implemented through a multi-layered approach that starts at the beginning when power is applied, establishes a trusted computing baseline, and anchors that trust in something that cannot be tampered with [6].

Security must be addressed throughout the device lifecycle, from the initial design to the operational environment:

1) Secure booting:

When power is first introduced to the device, the authenticity and integrity of the software on the device is verified using cryptographically generated digital

DOI 10.17148/IJARCCE.2015.412117

signatures. In much the same way that a person signs a check or a legal document, a digital signature attached to the software image and verified by the device ensures that only the software that has been authorized to run on that device, and signed by the entity that authorized it, will be loaded.

2) Access control:
Next, different forms of resource and access control are applied. Mandatory access controls built into the OS limit the privileges of device components and applications so they access only the resources they need to do their jobs. If any component is compromised, access control ensures that the intruder has as minimal access to other parts of the system as possible.
The principle of least privilege dictates that only the minimal access required to perform a function should be authorized in order to minimize the effectiveness of any breach of security.

3) Device authentication:
When the device is plugged into the network, it should authenticate itself prior to receiving or transmitting data. Just as user authentication allows a user to access a corporate network based on user name and password, machine authentication allows a device to access a network based on a similar set of credentials stored in a secure storage area.

4) Firewalling and IPS:
The device also needs a firewall to control traffic that is destined to terminate at the device. Deeply embedded devices have unique protocols, distinct from enterprise IT protocols. For instance, the smart energy grid has its own set of protocols governing how devices talk to each other.
The device needn't concern itself with filtering higher-level, common Internet traffic—the network appliances should take care of that—but it does need to filter the specific data destined to terminate on that device in a way that makes optimal use of the limited computational resources available.

5) Updates and patches**:**
Once the device is in operation, it will start receiving hot patches and software updates. Operators need to roll out patches, and devices need to authenticate them, in a way that does not consume bandwidth or impair the functional safety of the device.
Software updates and security patches must be delivered in a way that conserves the limited bandwidth and broken connectivity of an embedded device and eliminates the possibility of compromising functional safety.
Building security in at the OS level takes the responsibility off device designers and developers to configure systems to mitigate threats and ensure their platforms are safe

Security cannot be thought of as an add-on to a device, but rather as integral to the device's reliable functioning. Software security controls need to be introduced at the operating system level, take advantage of the hardware security capabilities now entering the market, and extend up through the device stack to continuously maintain the trusted computing base.

Security at both the device and network levels is critical to the operation of IoT. The same intelligence that enables devices to perform their tasks must also enable them to recognize and counteract threats. Fortunately, this does not require a revolutionary approach, but rather an evolution of measures that have proven successful in IT networks, adapted to the challenges of IoT and to the constraints of connected devices [7].

V. TECHNOLOGIES

Technologies are used in IoT to identify the thing, collect the data from thing, transmit that data over the internet, storing that data and giving back the collected data whenever request is made. Some of the technologies used in IoT are:

A. Radio-Frequency Identification(RFID)
Radio frequency identification is a technology to record the presence of object using radio signals. RFID is used for automatically identifying a person or an item. RFID systems consist of reading device called a reader and one or more tags. Reader has memory and computational resources. In tags there are different categories-Passive tags, Semi-Passive tags, Active tags. Passive tags-have limited computational capability, no ability to sense the channel, detect collisions and communicate with each other, Semi-Passive-consists of on-board power source that can be used to energize the microchip, Active tags-can sense the channel and detect collisions. It is more reliable, efficient, secured, inexpensive and accurate. FID is extensively used in automobile ignition keys, credit cards, passports which are called as RFID enabled passports etc.

B. Internet Protocol(IP)
Internet Protocol is a communication protocol. The Internet Protocol is responsible for addressing hosts and for routing datagram's (packets) from a source host to a destination host across one or more IP networks. For this purpose, the Internet Protocol defines the format of packets and provides an addressing system. The two versions of Internet Protocol (IP) are in use: IPv4 and IPv6. Each version defines an IP address differently. There are five classes of available IP ranges in IPv4: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used.IPv6 is the most recent version of the Internet Protocol.IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address.IPv6 uses a 128-bit address, allowing 2128, or approximately 3.4×1038 addresses, or more than 7.9×1028 times as many as IPv4, which uses 32-bit addresses and provides approximately 4.3 billion addresses.

C. Electronic Product Code (EPC)
The Electronic Product Code (EPC) is designed as a universal identifier that provides a unique identity for every physical object. Before IP address, EPC was used to identify the device uniquely. It is a standard that seeks to provide unique identification for RFID tags. It was originally created by MIT's Auto-ID Center and is currently directed by EPC global, an organization

dedicated to the global standardization of EPC. The EPC global stack is the de facto standard for retail and consumer goods industries.EPC is 64- or 96-bit code based on current numbering schemes (Global Trade Item Number [GTIN], etc.) containing a header to identify the length, type, structure, version, and generation of the EPC, the manager number, which identifies the company or company entity, the object class.

D. Cloud Computing

As we are generating a lot of data this data needs to stored somewhere. This is where cloud computing is more useful. Cloud computing as a paradigm for big data storage and analytics. While the Internet of Thing is exciting on its own that the real innovation will come from combining it with cloud computing. The combination of cloud computing and IoT can enable sensing services and powerful processing of sensing data stream. For example, the sensing data to be stored allowed by cloud computing and it used intelligently for smart monitoring and actuation with the smart devices. Cloud computing offers their services as-Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS).

Infrastructure as a service (IaaS)-In the most basic cloud-service model - and according to the IETF (Internet Engineering Task Force) - providers of IaaS offer computers – physical or (more often) virtual machines – and other resources.

Platform as a service (PaaS)-In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming-language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying.

Software as a service (SaaS)-In the software as a service (SaaS) model, users gain access to application software and databases.

E. Zigbee

ZigBee is open, global wireless standard to provide the foundation for the Internet of Things by enabling simple and smart objects to work together and thus improving comfort and efficiency in everyday life.

ZigBee is a specification for a suite of high-level communication protocols used to create personal area networks built from small, low-power digital radios. ZigBee is based on an IEEE 802.15.4 standard. Its low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics. ZigBee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. ZigBee is typically used in low data rate applications that require long battery life and secure networking [8].

VI. ADVANTAGES AND DISADVANTAGES

A. Advantages

IoT devices are designed to help consumers save money, reduce energy, and eliminate some hassles of everyday life by providing automation, efficiency, safety, and convenience which can help individuals, businesses, and society on a daily basis. The services offered by IoT can improve decision making and outcomes in a wide range of application areas.When implemented correctly, the Internet of Things can bring major business benefits, including boosted productivity and competitive advantage.

IoT present's organizations with tremendous opportunities to create innovative products and services, drive down operational costs and serve up additional revenue streams. The actual value of the IoT lies in integrating data produced by devices with business processes to optimize critical functional areas and improve operational performance.

The IoT allows to automate and control the tasks that are done on a daily basis, avoiding human intervention. It leads to uniformity in the tasks and good quality of service. Machine-to-machine interaction helps to maintain transparency in the processes and provide better efficiency. Hence, accurate results can be obtained rapidly which helps in saving valuable time. Instead of repeating the same tasks every day, it enables people to do other creative jobs. It is also beneficial in taking necessary actions in case of emergencies.

Adopting this technology and keeping these smart devices under surveillance, energy and resource utilization can be optimized efficiently contributing to the society. In addition, possible bottlenecks, breakdowns, and damages to the system can be avoided substantially. Hence, one of the major advantages of IoT is saving money

All the applications of this technology culminate in increased comfort, convenience, and better management, thereby improving the quality of life

B. Disadvantages

The Internet of Things (IoT) is revolutionizing our everyday lives.

As consumers are increasingly drawn to the conveniences, ease and benefits of IoT devices, most are unaware of the risks associated with it. The main concerns that accompany the Internet of Things are the breach of privacy, security risk, over-reliance on technology, and the loss of jobs.

IoT relies on an Internet connection to gather and analyse data, and it can be controlled by any suitable gadget. As with any Internet-connected device, IoT appliances and gadgets have potential security vulnerabilities. As a result, personal data and privacy of the consumers are at risk even without their knowledge. IoT devices including smart TV's, network routers, and even refrigerators are prone to cyber-attacks.

An August 2014 study from Hewlett-Packard found that 70 percent of all IoT devices are vulnerable to being hacked. The study examined 10 smart devices and found that each had about 25 potential vulnerabilities.

If an IoT device is affected by malware or threats, your PC or smartphone which is on the same network is highly prone to get infected if it is not secured with appropriate/requisite firewall and antivirus protection.

Furthermore, relying on technology completely on a day to

Day basis and making decisions according to the information it provides could be pernicious. Technologies involving internet are constantly prone to glitches as no system is robust and fault-free. Depending on the amount that an individual relies on the information supplied could be detrimental if the system collapses and in that case it may lead to a potentially catastrophic event.
The IoT is a diverse and complex network. Any failure or bugs in the software or hardware will have serious consequences.
Another major concern is, the automation of IoT will have a devastating impact on the employment prospects of less-educated workers which may lead to unemployment and ultimately affect the society as a whole [9].

VII. CONCLUSION

The internet of things might seem daunting to some people– too close to an automated, robotic world. But the reality is that we've already begun to automate as many aspects of the workplace as possible, and the home is just the next step. The internet of things simply allows humans to focus on larger prospect than the smaller tasks which can be taken care of by machines too.
Internet of Things is a technology in which the virtual world of information technology meets the real world of things making our life become better and more comfortable.

In conclusion, IoT represents the next evolution of the Internet. Given that humans advance and evolve by turning data into information, knowledge, and wisdom, IoT has the potential to change the world as we know it today—for the better.

ACKNOWLEDGMENT

This research was supported by the Computer Science Department, Muffakham Jah College of Engineering & Technology. We thank our institution who provided insight and support that greatly assisted the research.

We are immensely grateful to **Mr. Mir Ahmed Ali** for assistance with his knowledge, expertise and experience that greatly improved the manuscript.

We also express our deep gratitude to **Dr. A.A. MoizQyser,** H.O.D, CSE dept. for sharing his pearls of wisdom with us during the course of this research. Although any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

[1] Shancang Li & Li Da Xu &Shanshan Zhao, "The internet of things: a survey" 26 April 2014.
[2] Andrew Whitmore & Anurag Agarwal & Li Da Xu, "The Internet of Things—A survey of topics and trends" 12 March 2014.
[3] CharithPerera, ArkadyZaslavsky, Peter Christen, and DimitriosGeorgakopoulos, "Context Aware Computing for The Internet of Things: A Survey", Vol. 16, No. 1, First Quarter 2014.
[4] SomayyaMadakam, R. Ramaswamy, SiddharthTripathi, "Internet of Things (IoT): A Literature Review".
[5] OvidiuVermesan, Peter Friess, "Internet of Things- From Research and Innovation to Market Deployment".
[6] Teng Xu, James B. Wendt, and MiodragPotkonjak, "Security of IoT Systems: Design Challenges and Opportunities".
[7] Wind River Systems Inc., "Security in the internet of things", 2015.
[8] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, MarimuthuPalaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", 24 February 2013.
[9] Arpita R, Karan Saxena& Amit AsishBhadra, "Internet of Things" Volume 01, No.4, April 2015.