IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. V (Sep.- Oct. 2017), PP 57-65
www.iosrjournals.org

Solutions of common challenges in IoT

AmathulHadiShakara[1], Md. TareqHasan[2],
NadiaAkter[3]1DepartmentofElectronicandTelecommunicationEngineering,UniversityofDevelopmentAlternative,Bangladesh2,3DepartmentofComputerScienceandEngineering,UniversityofDevelopmentAlternative, Bangladesh

Abstract: *With the development of technology in modern science, the world has become smaller and easier to us. Today, internet is being used not only on personal computers but also on various smart devices. Smart devices can be considered as interactive electronic devices where they connect with other smart devices through a network to share and interact remotely. Internet of Thing is this kind of invention of modern science which is a computing technology provides anetwork of things and people where human and devices with sensor can communicate each other to perform many different tasks of our day to day life.This paper provides an overview of the Internet of Things (IoT)and its architecture emphasis on well-known problems of IoTandits possible solutions.This paper encountered the discussion of IoT architecture problems and many other challenges including the new malware attack, also proposing some solutions ofscalability, latency, bandwidth, malware attack including RFID and NFC problem.*

Date of Submission: 14-10-2017 Date of acceptance: 04-11-2017

I. Introduction

In 1995, only 1% people of world population used internet. But today 47% of the world population has an internet connection. Usage of internet is increasing rapidly.With the rising percentage of internet usage, number of smart devices in the market also is increasing and researchers estimate that by 2020, the number of active connected smart devices will exceed 40 billion.

The term Internet of Things abbreviated as IoT first coined by British researcher Kevin Ashton in 1999:

"*I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. It summed up an important insight which is still often misunderstood.*"[1]

While speaking at Fortune's Global Forum last monthKevin Ashton predicted that, 500 billion devices would be connected to the internet by 2025. (This prediction massively exceeds other predictions estimated by various stakeholders.)Take BI Intelligence,for example, which estimates that the number of IoT devices will hit 34 billion by 2020. Tech research firm, Gartner, which conservatively pegs it at 21 billion devices [2] .So 500 billion, is a particularly headline-grabbing number. Well, whether it's 21 billion, 34 billion, or 500 billion, it doesn't matter. (For instance if we take Business Intelligence as an example, it estimates IoT device will reach 34 billion and Gartner (tech research firm) argues that the number will be 21 billion devices. Irrespective of the number to be reached all the stakeholders predict a rise in the IoT connected devices.

The Internet of Things is going to increase exponentially as more devices get smarter and more consumers get tech savvy.Gartner predicts that, by 2020, the IoT market will be comprised of 20.8 billion things—up from 6.4 billion connected things in 2016[2].Experts estimate that the IoT will consist of about 30 billion objects by 2020.

II. IoT Architecture

IoT architecture is mainly based on an open model using open protocols, in order to support existing network protocols.There is no single consensus on architecture for IoT, which is agreed universally. Different architectures have been proposed by different researchers.

[**https://www.hindawi.com/journals/jece/2017/9324035/**]The most basic architecture is three-layer architecture [3–5] as shown in Figure 1. It was introduced in the early stages of research in this area. It has three layers namely,

i. Perception
ii. Network and
iii. Application layers.

These are discussed further in details:

i. The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.
ii. The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.
iii. The application layer is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities and smart health.

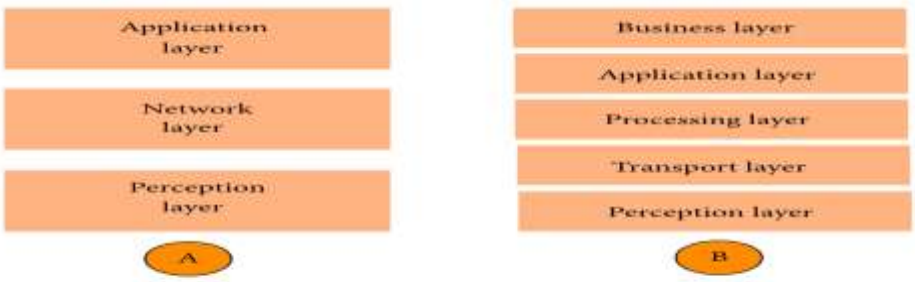


Figure 1: Architecture of IoT (A: three layers) (B: five layers).

The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the five-layer architecture, which additionally includes the processing and business layers [3–6]. The five layers are perception, transport, processing, application, and business layers (see Figure 1). The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers.

(i) The transport layer transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.
(ii) The processing layer is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.
(iii) The business layer manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further.

Another architecture proposed by Ning and Wang [7] is inspired by the layers of processing in the human brain. It is inspired by the intelligence and ability of human beings to think, feel, remember, make decisions, and react to the physical environment.

It is constituted of three parts. First is the human brain, which is analogous to the processing and data management unit or the data center. Second is the spinal cord, which is analogous to the distributed network of data processing nodes and smart gateways. Third is the network of nerves, which corresponds to the networking components and sensors.

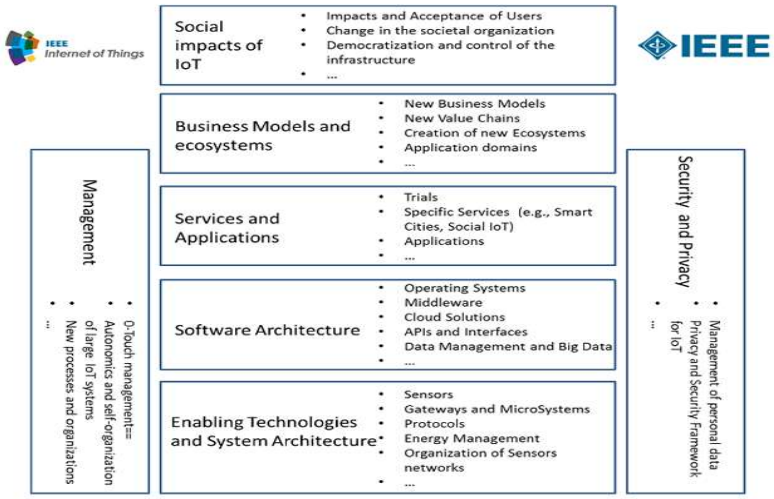


Figure 1. Technological and social aspects related to IoT

III. IoT Challenges

Despite IoT's benefits and its effort to make daily life more comfortable pressing issues remain regarding the use of this technology. The issues include:

1. Security
2. Privacy
3. Interoperability/ Standards
4. Legal, regulatory and rights
5. IoT Architecture problem
6. Scalability
7. Latency
8. Quality of Service (QoS)

The limitations are described below:

3.1 Security:

Ensuring security in IoT products and services must be a fundamental priority. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Poorly secured IoT devices and services can serve as potential entry points for cyber-attack and expose user data to theft by leaving data streams inadequately protected.

The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally.

As a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the Internet itself to potential harm. Accordingly, a collaborative approach to security will be needed to develop effective and appropriate solutions to IoT security challenges.

(i) RFID and NFC technology:

Within the IoT environment, RFID (Radio Frequency Identification) technology is used mostly for the automated information exchange. Due to known security disadvantages of this technology there are a number of assumed threats. The lack of adequate authentication mechanisms in a number of RFID tags allows unauthorized access to their contents. Although the content of the tag is not easy to read, the unauthorized alteration of its content or its deletion is very possible. The attack on the availability of RFID tags can be carried out through a DoS attacks. DoS attack causes the failure of transmission of identification information stored in the tags.

Threats against the confidentiality of the data include attacks such as tag monitoring with the use of an unauthorized reader which can result in the interception of sensitive information such as street addresses, phone numbers, and identification tags. Attacks on the data integrity are related to unauthorized tag cloning with the use of unauthorized readers which allow cloning in order to bypass implemented protection methods. In addition to these threats, environments using RFID technology are also vulnerable on eavesdropping, MitM attacks, spoofing, and others.

NFC (Near Field Communication) technology is different from RFID in used frequency range and connection topology. The technology is based on the principles and the relations between magnetism and the electricity, or on the principles of the inductive loop. Although short-range, NFC technology is vulnerable to many threats such as eavesdropping, unauthorized manipulation of data and MitM attacks. Although eavesdropping and MitM attack methods are considered less risky, these attacks are possible with the use of the expansion method of communication range up to 10 meters in the active communication mode and up to one meter in the passive communication mode.

(ii) Bluetooth technology:

Bluetooth is a wireless communication technology for short-range communication. The technology enables the creation of Adhoc, piconet, network between two or more devices and has implemented protection methods that are based on authentication and encryption. There are four modes of protection (Security mode 1, Security mode 2, Security mode 3 and Security mode 4). Mode 1 does not require authentication and encryption, mode 2 applies authentication and encryption exclusively for individual services such as data transfer, mode 3 forces authentication, and encryption before the connection with the device is established, and mode 4 uses a simple method of pairing with the aim of establishing security on the service level.

The threat classification of the Bluetooth technology is presented in where the threats are classified into nine categories. Each threat is different; therefore each one is assigned to a threat level category.

(iii) ZigBee technology:

The ZigBee technology plays an important role in the formation of WSN (Wireless sensor network) because of advantages such as low cost, high reliability, low complexity and variety of application in the IoT environment. The advantages of this technology are the autonomy, flexibility, scalability and low cost of the devices. Despite the offered advantages, a large number of security threats are oriented against specified data transmission technology.

Some of the known security threats of the ZigBee technology are the unauthorized traffic gathering, packet decoding and data manipulation. For example, unauthorized access to a sensor node within a ZigBee network gives access to the shared secret key of the network and thus the traffic within the network. In addition to known threats, new threats appear, such as the sabotage of terminal devices in the ZigBee network with the purpose of the exhaustion of the battery capacity and the exploitation of the key exchange process.

(iv) 6LoWPAN technology:

IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is a communication technology that enables connectivity of the hardware limited devices (sensors, actuators, etc.) onto IPv6 network through the IEEE 802.15.4 standard. This communication technology has an increasing role in the IoT environment due to the high presence of devices with limited processing, memory, and the other features. This technologyalso has a large number of vulnerabilities and threats that have the potential of their exploitation.

(v) Malware attack:

MIRAI – possibly the biggest IoT-based malware threat that emerged in 2016, which caused vast internet outage in October 2016 by launching massive distributed denial-of-service (DDoS) attacks against the popular DNS provider Dyn. Now, the infamous malware has updated itself to boost its distribution efforts. Researchers from Russian cyber-security firm Dr.Web have now uncovered a Windows Trojan designed to build with the sole purpose of helping hackers spread Mirai to even more devices. Mirai is a malicious software program for Linux-based internet-of-things (IoT) devices which scan for insecure IoT devices, enslaves them into a botnet network, and then used them to launch DDoS attacks, and spreads over Telnet by using factory device credentials. It all started early October 2016 when a hacker publicly released the source code of Mirai. Dubbed Trojan.Mirai.1, the new Trojan targets Windows computers and scans the user's network for compromisable Linux-based connected devices. Once installed on a Windows computer, the Trojan connects to a command-and-control (C&C) server from which it downloads a configuration file containing a range of IP addresses to attempt authentication over several ports such as 22 (SSH) and 23 (Telnet), 135, 445, 1433, 3306 and 3389. Successful authentication lets malware runs certain commands specified in the configuration file, depending on the type of compromised system. In the case of Linux systems accessed via Telnet protocol, the Trojan downloads a binary file on the compromised device, which subsequently downloads and launches Linux.Mirai. "Trojan.Mirai.1's Scanner can check several TCP ports simultaneously. If the Trojan successfully connects to the attacked node via any of the available protocols, it executes the indicated sequence of commands," claimed the company in an advisory published this week. Once compromised, the Trojan can spread itself to other Windows devices, helping hackers hijack even more devices. Besides this, researchers noted that the malware could also identify and compromise database services running on various ports, including MySQL and Microsoft SQL to create a new admin “phpminds” with the password a “phpgodwith,” allowing attackers to steal the database. At this time it’s not known who created this, but the attack design demonstrates that your IoT devices that are not directly accessible from the internet can also get hacked to join the Mirai botnet army.

All it takes is the hundreds of millions of unsecured shoddy devices of the Internet of Things (IoT). In the Dynonslaught , Kyle York, Dyn's chief strategy officer said the DDoS attack used "tens of millions" devices. Hangzhou Xiongmai Technology, a Chinese technology company, has admitted that its webcam and digital video recorder (DVR) products were used in the assault. Xiongmai is telling its customers to update their device firmware and change usernames and passwords. The attack itself appears to have been made with the Mirai botnet. This open-source botnet scans for devices using their default username and password credentials. Jeff Jarmoc, a Salesforce security engineer, tweeted, "In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters." [13]

3.2 Privacy:

The full potential of the Internet of Things depends on strategies that respect individual privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users, but concerns about privacy and potential harms might hold back full adoption of the Internet of Things. This means that privacy rights and respect for user privacy expectations are integral to ensuring user trust and confidence in the Internet, connected devices, and related services.

Indeed, the Internet of Things is redefining the debate about privacy issues, as many implementations can dramatically change the ways personal data is collected, analyzed, used, and protected. For example, IoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to out of certain data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of users.While these are important challenges, they are not insurmountable. In order to realize the opportunities, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services.

Many new industry coalitions have emerged alongside traditional Standards Developing Organizations (SDOs) to increase efforts to assess, develop, modify, or harmonize standards and protocols related to IoT. This includes, for example, long-standing SDOs such as the IETF, ITU, and IEEE, and comparatively new efforts such as the Industrial Internet Consortium, Open Interconnection

3.3 Interoperability/Standards:

A fragmented environment of proprietary IoT technical implementations will inhibit value for users and industry. While full interoperability across products and services is not always feasible or necessary, purchasers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, and concern over vendor lock-in.

In addition, poorly designed and configured IoT devices may have negative consequences for the networking resources they connect to and the broader Internet. Appropriate standards, reference models, and best practices also will help curb the proliferation of devices that may act in disrupted ways to the Internet.

3.4 Legal, Regulatory and Rights:

The use of IoT devices raises many new regulatory and legal questions as well as amplifies existing legal issues around the Internet. The questions are wide in scope, and the rapid rate of change in IoT technology frequently outpaces the ability of the associated policy, legal, and regulatory structures to adapt.

One set of issues surrounds cross border data flows, which occur when IoT devices collect data about people in one jurisdiction and transmit it to another jurisdiction with different data protection laws for processing. Further, data collected by IoT devices is sometimes susceptible to misuse, potentially causing discriminatory outcomes for some users. Other legal issues with IoT devices include the conflict between law enforcement surveillance and civil rights; data retention and destruction policies; and legal liability for unintended uses, security breaches or privacy lapses.

3.5 IOT architecture problem:

The IoT environment should be capable of interconnecting large number of heterogeneous objects through the Internet. So, there is a need for elastic and adjustable layered architecture. The general IoTarchitecture is divided into three layers such as Perception layer, Network Layer and Application layer. Figure.1 shows the three-layer IoT architecture.

i. Perception Layer

This layer collects information through the sensing devices such as RFID, Zigbee and all kinds of sensors. Radio Frequency Identification (RFID) technology enables the design of microchips for wireless data communication and helps in automatic identification of anything they are attached to, acting as an electronic barcode. The collected data are transmitted only through wireless network transmission (WSN). Some common attacks that occur in this layer are: Node capture, Fake node or malicious data, Denial of Service attack, Reply attack etc.

Devices of the perception layer are often limited in terms of process and data storage resources, and the applied technologies (such as RFID/NFC, Bluetooth, ZigBee and 6LoWPAN) are being limited in data transmission range and rate. Restrictions are imposed in order to achieve greater autonomy, reduce physical dimensions and increase the flexibility of such devices, but also to reduce the final cost of such devices.

Table 1. Transmission technology features of the perception layer [10]

Features/Technology	NFC	RFID	Bluetooth	ZigBee	6LoWPAN
Coverage Area	PAN	PAN	PAN	LAN	LAN
Topology	P2P	P2P	Star	Mesh/Star/Tree	Mesh/Star
Power consumption	Very Low	Very Low	Low	Very Low	Very Low
Speed	400 Kbps	400 Kbps	0,7 - 1 Mbps	250Kbps	250Kbps
Range	< 10 cm	< 3 m	5 - 30 m	10 - 300m	800 m

Basic features of each transmission technology, such as the coverage, topology, power consumption, data transmission rate and range, are shown in Table 1. Perception layer is specific in the IoT environments, opposed to the other layers which are in some form present in other information and communication environments.

ii. **Network Layer**

This layer supports secure data transfer over the sensor networks and responsible for routing. It transfers the information through wireless technology such as Wi-Fi, Bluetooth, and Infrared etc. Hence, this layer is mainly responsible for transferring the information from perception layer to upper layer. There are some common security problems in LAN, Wi-Fi, and Internet. They are: illegal access network, eavesdropping information, confidentiality and integrity damage, DoS attack, Man-in-the-middle attack etc.

iii. Application Layer

This layer is the topmost layer of the IoT architecture that provides the delivery of all services in various fields. It includes cloud computing, intelligent transportation, environmental monitoring etc. Application layer has some security problems such as data security, cloud platform security, data protection and recovery etc. To solve the security problems of this layer, authentication and privacy protection are needed. Particularly, password management is very important for data security.

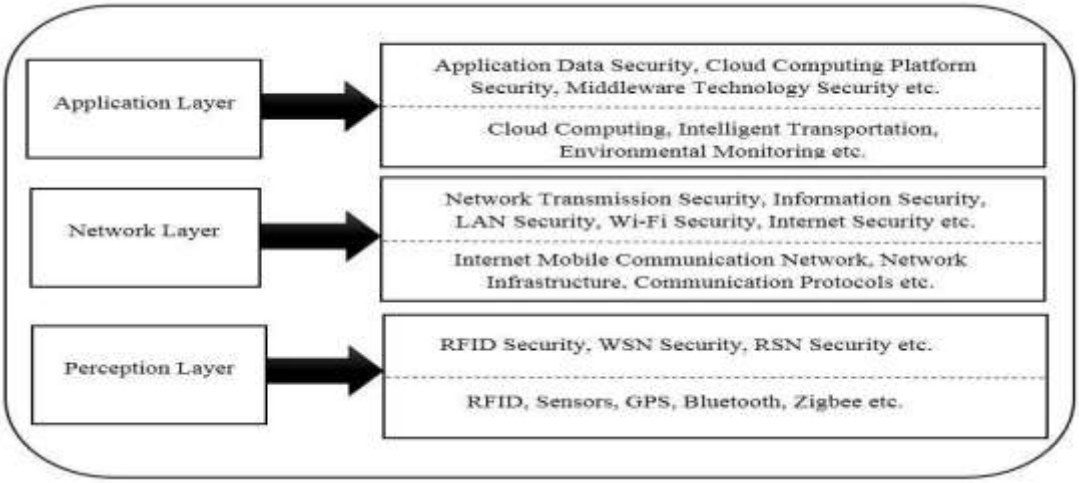


Figure 1: Three-layer IoT Architecture [11]

4.6 Scalability:

By 2020, Cisco estimates 50 billion **[40]** devices will be connected to the cloud, while Gartner estimates 26 billion [52]. Scalability in the IoT spaces will be more challenging than web-scale or Internet-scale applications; the amount of data generated will easily ex-ceed the reported trillion objects in Amazon S3.**[12]**

4.7 Latency:

Latency is the time it takes data to travel across the network. Usually, latency is measured as an RTT, or round-trip time: this is the time a packet takes to get from source to destination and back. Within the data center, latency is measured in milliseconds (ms) and is generally in the less than 5 ms range. Recently IOT environment capable of interconnecting large number of heterogeneous objects through the Internet. More devicesmean more latency because the network became heavy. Application developers view the cloud as a component that interconnects the smart devices. However, from a network point of view, the cloud is on the edge of the network. Even simple IoT applications, such as those that turn on a fan in response to a rise of the local temperature, will experience unpredictable latencies from sensing, wireless transmission, gateway processing, Internet delivery, and cloud processing.

4.8 Quality of Service (QoS): Web users tolerate variable latency and occasional loss of web services. In contrast, the temporary unavailability of sensors or actuators within IoT applications will directly impact the physical world. While significant engineering effort has been put into improving the availability and latency pro-file of the cloud (allowing Service Level Agreements), such efforts are stymied by operator error, software bugs, DDoS attacks, and normal packet-to-packet variations from wide-area routing. Further, the Internet connection to people's homes is far from perfect. Over 10% of home networks in the developed world see connectivity interruptions more frequently than once every 10 days this situation is worse in developing countries.

IV. Proposed Solution

4.1 RFID and NFC technology:

Table 2. Threats and the proposed solution for the RFID and NFC technology

Threats	Method of protection	Technology	Description
Tag Cloning	Syncronized secrets method	RFID	Synchronized secrets method that can detect cloning attacks and pinpoint the different tags with the same ID
Information leakage	RFID-Tate	RFID	Light-weight identity protection and mutual authentication using Identity-based Encryption (IBE) method.
Eavesdropping, tag Cloning	OTP authentication	RFID	Method uses dynamic password and backend system authentication methods. It can effectively prevent the security vulnerabilities such as dictionary attacks, replay attacks, data eavesdropping and tags forgery.
Evesdropping, location Tracking, replay attack, MitM, De-Syncronization Attack	VLFSR lightweight encryption function	RFID	Security method is successful against the large scale of attacks on RFID. It can be used in design of secure RFID protocol with efficient hardware requirements to meet the demand of secure low- cost RFID systems or WSN.
Identity theft, Information leakage	Conditional privacy protection method	NFC	Proposed method can provide conditional privacy with less overhead, it can also hide user's identity, and its identity can be confirmed by the TSM (Trusted Service Manager).
Eavsdropping	Random key agreement method	NFC	Practical and energy efficient key agreement method for duplex

Table 2 presents some of the developed methods applicable to the protection of RFID and NFC technology within the IoT environment. Methods have been developed taking into account the specifics, or disadvantages of RFID and NFC technology.

4.2 Malware:

Securing the Internet of Things First, and this unfortunately is a long-term solution, IoT vendors must make it easy to update and secure their devices. ***Patching*** must be made mandatory and done automatically. One easy way to do this is to use an operating system, such as Ubuntu with Snap, to update devices quickly and cleanly. These "atomic" styles updating systems make patches both easier to write and deploy.

Another method is to ***lock down***IoT applications and operating systems. Just like any server, the device should have the absolute minimum of network services. Defending intranet and websites first, should protect sites by practicing DDoS prevention 101. For example, make sure routers drop junk packets. Should also block unnecessary external protocols such as Internet Control Message Protocol (ICMP) at network's edge. And, as always, set up good firewalls and server rules.

As Carl Herberger, vice president told Bloomberg, DNS providers are like hospitals: They must admit anyone who shows up at the emergency room. That makes it all too easy to overwhelm them with massive in the range of 500 gigabits per second -- attacks. In short, there is no easy, fast fix here. One way you can try to keep these attacks from being quite so damaging is to increase the Time to Live (TTL) in your own DNS servers and caches. Typically, today's local DNS servers have a TTL of 600 seconds, or 5 minutes. If you increased the TTL to say 21,600 seconds, or six hours, your local systems might dodge the DNS attack until it was over.

4.3 Scalability:

Internet of Things (IOT) opportunities presents unique technical challenges, requiring solutions that are reliable, flexible, secure and scalable. As the technology leader in data management, Oracle's IoTPlatform provides effective solutions for this connected new world. Oracle products are combined together in integrated application architecture, providing a comprehensive set of solutions to address those challenges.

In this session, we focus on the integration of data received from all the different devices and components of an Internet of Things (IoT) ecosystem. Oracle Database Mobile Server and Oracle NoSQL Database work together to provide a reliable, flexible, secure and scalable solution to the problem of IoT data ingestion and management. Oracle Database Mobile Server, the best way to securely connect embedded devices and mobile applications to Oracle Database Oracle NoSQL, a distributed, highly reliable, scalable and available key-value database.

4.4 Latency:

The issue of latency is becoming increasingly complex. In order to leverage cloud computing as a true business enabler, it is critical that organizations learn how to manage and reduced.The first step in reducing latency is to identify its causes. To do this, we must examine latency not as it relates to the web, but as it relates to the inherent components of cloud computing.

Distributed computing is one component adding to cloud latency's complexity. With enterprise data centers a thing of the past, the nature of applications has completely changed from being contained within a local infrastructure to being distributed all over the world. The proliferation of Big Data applications using tools such as R and Hadoop are incentivizing distributed computing. Furthermore, latencies are entirely dependent on Internet traffic, which waxes and wanes to compete for the same bandwidth and infrastructure.

Another complexity layer lies in the lack of measurement tools for modern applications. While ping and trace route can be used to test Internet connection, modern applications don't have anything to do with ICMP, the protocol behind these tracing devices. Instead, modern applications and networks use other protocols such as HTTP and FTP and therefore need to try to measure their performances accordingly.

Prioritizing traffic and Quality of Service (QoS) delve deeper into cloud latency's complexity. Pre-cloud, Service Level Agreements (SLAs) and QoS were created to prioritize traffic and to make sure that latency-sensitive applications would have the network resources to run properly. However, cloud and virtualized services make this a dated process, given that we need to now differentiate between certain items like an outage in a server, a network card, a piece of the storage infrastructure, or a security exploit. Different cloud applications have different tolerances for network latency, depending on their level of criticality; while an application controlling back-office reporting may tolerate lower uptime, not all corporate processes can allow for downtime without having a significant impact on the business. This makes it increasingly important for SLAs to prioritize particular applications based on performance and availability.

Despite latency's complexity, it provides a great opportunity for innovative cloud-based solutions, such as the Radar benchmarking tool from Cedexis, which provides insight into what goes on across various IaaSproviders, as well as tools like Gomez, which are helpful in comparing providers. While tools are of course helpful in providing insight on trends, the overarching solution to measuring and mitigating cloud latency is providing more consistent network connections.

The best available option is to connect to a public cloud platform. Amazon's Direct Connect is the best that we've seen in providing more predictable metrics for bandwidth and latency. Another viable option is Windows Azure – both products are particularly useful for companies looking to build hybrid solutions, as they allow some data to be stored on premise while other solution components can be migrated to the cloud.

Finally, by collocating within a third-party data center, companies can rest assured that their cloud applications are equipped to handle all of latency's challenges and reap extra benefits in terms of monitoring, troubleshooting, support, and cost. Colocation facilities that offer specific Cloud Hubs can provide excellent connectivity and cross-connections with cloud providers, exchanges and carriers that improve performance and reduce latency to end users. Furthermore, colocation data centers ensure that companies not only have the best coverage for their business, but also a premium network at their fingertips.

4.5 Bandwidth:

If you have more IoT devices trying to report data over a low bandwidth link than it is capable of carrying, then to ensure that the most important data gets through you are going to have to filter out the less important data, and compress the remaining data down. Hopefully the data will then fit within the available bandwidth. Life is full of comprises, and the lack of bandwidth forces you to make some of the hardest ones.

4.6 QoS:

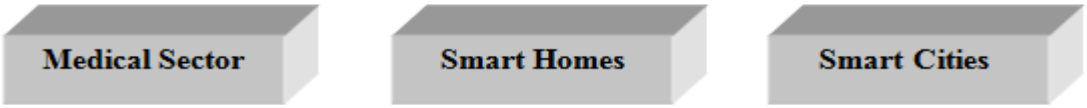
The soaring number of connected objects represents a massive opportunity for mobile operators. But for success with applications in the Internet of Things, reliable and trusted connectivity is essential. GemaltoIoT Quality of Service is a comprehensive offer for mobile operators to monitor the cellular connectivity of smart static and mobile objects in real time.

Suited to a wide range of IoT use cases including automotive, smart metering, smart home and connected Point-of-Sale applications, the solution provides instant network status and analysis. In addition, it immediately highlights issues by ensuring that a rich array of data is readily accessible.

Future Scope

With the passage of time, people around the globe are now more inclined to technology rather than manual approach and everyone wants their job to be done for them with minimal effort. In simple terms we can say, Internet of things are computing devices which sends and receives data over the internet.

The benefits of IoT are providing people a level of comfort which is making IoT an important part of their lives. IoT can help people around the globe in the following areas:



i. **Medical sector:** A wide level of implementation can be done. Tele-medicine, checkups, health devices (wearable) and many more.

ii. **Smart Homes:** A number of devices have been introduced from Google - Google Home, Amazon- Alexa, Nest and there are many of them which serve one or the other purpose enabling the house hold to interact with each other over internet and make our lives easier than before.

iii. **Smart Cities:** The biggest problem in metropolitan cities are time killing traffic jams but IoT is making easier in connecting and information passing so that the situation can be handled beforehand. Advanced parking systems, Security systems.

There are many more sectors like Industrial Automation, the combination of Artificial Intelligence with IoT example: JARVIS made by Mark Zuckerberg, Manufacturing, Advanced power supply, planning, Digitization of cities in developing countries. The opportunities are endless.

Conclusion

References

[1] Source: http://www.rfidjournal.com/articles/view?4986, accessed in 10th May, 2017.
[2] http://www.gartner.com/newsroom/id/3165317
[3] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68–90, 2015.
[4] O. Said and M. Masud, "Towards internet of things: survey and future vision," International Journal of Computer Networks, vol. 5, no. 1, pp. 1–17, 2013.
[5] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China, August 2010.
[6] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT '12), pp. 257–260, December 2012.
[7] H. Ning and Z. Wang, "Future internet of things architecture: like mankind neural system or social organization framework?" IEEE Communications Letters, vol. 15, no. 4, pp. 461–463, 2011.
[8] *Nordrum, Amy (18 Aug 2016).* "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated". *IEEE.*
[9] *http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf*
[10] DAAM
[11] http://www.ijesmr.com/doc/Archive-2016/November-2016/5.pdf
[12] *Cloud Paper Reference*
[13] https://thehackernews.com/2017/02/mirai-iot-botnet-windows.html

AmathulHadiShakara, Md. TareqHasan, Nadia Akter, Solutions of common challenges in IoT." IOSR Journal of Computer Engineering (IOSR-JCE), vol. 19, no. 5, 2017, pp. 57-65.