Survey Paper for IOT, Capacity Planning and Cloud Technologies

Bhautik Pipaliya[1], Devanshi Gariba[2]

[1, 2]Ahmedabad University, Institute of Engineering and Technology, Ahmedabad, India

Abstract: ***As the world has already witnessed the huge transformation wave of Internet of Things ,it presents itself with a multitude of background technologies, seemingly appearing from nowhere. While Cloud computing and sophisticated security policies are the need of the hour, it brings about a zillion concerns and also proliferates business opportunities in such expanding domains. There exists a fine network fabric connecting all these technologies. Today's IOT scenario is still limited by design complexity, security and extensibility but the lines between analog and digital are sure to fade tomorrow. Exponential growth in data is an added complexity that is burdening almost all the already intricate information systems and work environments. Since the current forecast of 20-50 billion interconnected and programmed devices which will upgrade to cloud storage perhaps change into reality, these emerging technologies drive the need for enhanced capacity planning in network expansion for the internet of things as well as cloud technologies.***

Keywords: The Internet of Things, Ubiquitous Computing, Capacity Planning, Cloud Computing, Intricate Systems

1. Introduction

Mankind is progressing towards an era of artificial intelligence, which has developed over the years and its dogmatic nature compels the emerging technologies to smoothen the modern day living. With this persistent idea of making our everyday lives better, we have a whole raw concept of Internet of Things which can be analogous to an invisible robot that serves in mundane matters. However, having crossed the infancy stage, Internet of things is generating enormous amounts of data which has to be then processed and analyzed so that it becomes interpretable to embedded systems and humans. This is where data analytics fit in. However, it has to be dealt with in a very effective manner since it is then coining new problems of data security and data integrity. Now that ubiquitous computing is at zenith, there is an intense need for technologies to function around the ingestion of data from the physical world, giving way to dangerous data vulnerabilities that reside on clouds. These emerging technologies have observed global interest in recent years and there have been quite a lot of research and development progressing in these areas. Bigger firms, over the globe, have started investing a significant amount in these emerging technologies.

2. Various Technologies

2.1 Internet of Things

A Recent paradigm shift in the era of Pervasive computing is towards Internet of Things that operates on the similar cost of embedding processors in everyday objects and its interaction with humans and environment. According to the father of ubiquitous computing, this is the age of calm technology, when technology recedes into the background of our lives wherein billions of smart devices will be simulating in an environment, all the while sensing, interacting, and cooperating with one another to bring in tangible easiness to society. However, the technology has not yet matured enough for the markets to dynamically adapt. [6] In a recent survey of 561 executives worldwide by The Economist Intelligence Unit, results provided an account for the average business generated from using IoT in manufactured goods. Only 19IOT architecture can be visualized in units that are division into objects (things), gateways and network and cloud. Things that are considered for connectivity can be the most commonly used objects which can be connected directly through wireless networks to the internet. Gateways provide the needed establishment with cloud with added functionalities of security, connectivity and enablements. Virtual data centres and cloud infrastructures provide for large storage pools and servers that are internetworked as this technology continues to mature, it has already spawned a multitude of opportunities for industrial applications to be adopted in the market. From home automation systems, healthcare systems, home- security, transport sectors, business intelligence to military applications, a wide range of applications has started integrating IOT within. [1]

2.2 Security

Immense proliferation of IP-connected devices has given way to data privacy and security issues among potential consumers of devices and services that relate to Internet of things and pervasive computing. Also, as a matter of fact, one of the major reasons in hesitance in embracing cloud technology solutions and IOT solutions is data privacy which is significantly impacting their absolute willingness to adopt such technologies. Rising statistics in estimating that over 348 million identities were exposed through data breaches and that each day nearly 500,000 web attacks were blocked.[9] Device connectivity plays a critical role in ensuring security to users. However, it is worthy to notice that the most vulnerable device connectivity is Wi-Fi and perhaps it is due to the enormous compatibility of device types gaining access to a domestic or enterprise network. There definitely are WPA2 security protocols existing for personal and enterprise-grade routers, but hackers are rendering successful in challenging those as well. Also, there are potential risks posed by gateways, cloud-based applications and services, access networks. These risks again, have well presented themselves in the form of distributed denial of service (DDOS), which is an attempt to make an online service unavailable by over-burdening it with traffic load from various sources, targeting a wide variety of important resources, from banks to news websites. Smart devices are more often considered as DDoS attack sources. Moreover, there can be different ways of dealing with information security from DDos attacks. [5] The introduction of IPv6 can give service providers more opportunity to abate the risk of DDoS attacks and spoofed addresses. Also, Implementing a Cloud based DDoS mitigation architecture is essential in dealing with the risks of traffic spoofing on an IoT network. When we further look at identifying important traits of a secure network, it is important to realize that there is an extensive use of encryption during data transport and also in storing data locally. Encrypting data at the network level is certainly a must, but for emphasized security requirements, it is a good idea for encryption to be implemented at the data link level which follows from the fact that now an attack is less appealing to criminals because the data is essentially useless if a breach does occur. However, there is again a flip side on using encryption. It provides no protection against internal malicious attacks, for which again, non-cryptographic methods are introduced.

2.2 Performance Modeling and Capacity Planning

There are very few would not agree on keeping pace with the exponentially changing demands for typical products and the fact is that, organizations are always striving hard for determining their own production capacity. Moreover, Information Technology has especially always used supporting analytics tools on estimating the amount of hardware needed by the applications required by the organization. The most commonplace example that each one of us has definitely experienced is apology messages that show up on websites that are heavily loaded with unpredictable traffic due to which the site has to be upgraded with better services.[8]

Capacity planning deals with the creation of a baseline metric to comprehend the current utilization, followed by manually tracking new systems and analyzing utilization patterns that eventually help in forecasting future requirements. The main motivation of capacity planning is to ensure that enough capacity existed to avoid risks of failure at unexpected moments, thus controlling the dynamism and intricacy of systems used, which was perhaps missing a decade ago. Again, with the right tools, we can definitely locate and pinpoint underutilized capacity areas and urge the applications and subsystems to take advantage of that capacity, subsequently, delaying in the purchase of additional resources.

There are basic three Steps essential for Capacity Planning:

- Determine Service Level Requirements: It is always a good idea to categorize the work done by systems and to identify customer expectations for how that work gets done.
- Analyze Current Capacity: the Current capacity of systems should be analyzed to check whether it is keeping pace with customer needs.
- Forecast the future needs: After Analyzing the current business activity, future system requirements can be modeled with the stringent and compulsory implementation of the required changes in the system configuration that will ensure that sufficient capacity will be available to maintain service levels. In capacity planning, we keep enough room for circumstances to change Moreover, with the cloud, IOT, and big-data, transforming Information Technology completely; there is just an ever increasing burden on capacity planning. Determining exactly how a companys IT resources are being used over a period of time, gives them room, to adjust to actual user needs. This actually is the key to breaking the great inflationary power of overcapacity, and gaining an immense advantage over greater technical and financial headroom, clearly optimizing resource utilization by aligning lines with business motives and being a high-valued asset for business growth. It creates real value. Optimizing the operational cost and managing performance valuates any business organization.

2.4 Cloud Computing

Explosive growth in data is troubling almost every emerging discipline. Moreover, In the past few years, business Intelligence systems have evolved over software solutions that have started overwhelming typical hardware architecture. Business Intelligence solutions have now converted themselves into intricate business processes wherein they integrate software that is able to process and also provide custom built hardware as required. Now to adapt hardware architecture to various software solutions, operational costs of building and maintenance scales up. Thus, there is a need for cloud technologies that ensures elastic resource-sharing and metered services or pay per use. Then there are notions of public clouds and private clouds.

- **Public Clouds**
  Public clouds are managed by companies that offer access over a public network to affordable computing resources. The key aspect of public cloud is that customer's do not really have to purchase hardware, software or supporting infrastructure, which is owned and managed by providers. It then provides flexibility and scalability in terms of storage and computing services, but again comes with it privacy concerns which is then like a trade-off with cost.

- **Private Clouds**
  Private clouds resemble infrastructures that are operated solely individual organizations, and can be managed internally or by a third party, and be hosted either internally or externally. These are advantageous in terms of clouds efficiencies that provide for more control over in-demand IT resources, enhanced storage and analytics with sophisticated security policies designed for specific organizations need. Furthermore, cloud technologies can be further divided into Software as a service, Platform as a service and Infrastructure as a service.

- **Software as a Service(SAAS)**
  Cloud-based applications that run on distant computers

that can be connected to users computers via The Internet wherein data is available from any connected computer and all the data is already uploaded on the cloud.

- **Platform as a Service(PAAS)**
  It provides cloud-based environment for building and delivering the web-based application with eliminating the cost and complexities of buying and managing the underlying hardware, software, provisioning and hosting.
- **Infrastructure as a Service(SAAS)**
  It provides companies with multiple computing scalable resources which includes servers, networking, storage and data center space on a pay-per-use basis to support dynamic workloads which saves investment on hardware.

3. Issues and Challenges

3.1 Internet of Things and Security

Internet of Things (IoT) functions on integrating innumerable smart objects with the Internet connecting both the physical and the virtual worlds and brings with its significant complexities in terms of connectivity, communication, addressing, network management and most importantly, privacy and security. Furthermore, with cloud computing on ever-rising levels, there is an increasing pressure to protect sensitive information. With network expansion in almost each and every domain and increased mobile computing, they have presented mainly two security risks: Malicious apps (malware) and app vulnerabilities that arise when applications deployed by the organization gain access to corporate data contains security weaknesses.[7] Especially the applications with enhanced internet usage that store data on clouds are most vulnerable to data leakages. Some of the important privacy risks arise from web application vulnerabilities, storage of important bank details, operator-side data leakage through encryption, inadequate data breach response followed by data sharing between third parties not transparent to users and insecure data transfer. As IOT is an emerging technology, It yet lacks a common standard or protocol for its functioning. It is yet an important issue to be resolved since it is one of the invisible factors for its market adoption. As more and more organizations design IoT security controls, these may vary and also interfere with personal perspectives of privacy. There are different data protection regulations announced each day which vacillates an IOT user which ultimately leads to the slow market adoption of this huge industry. Thus, there is a need for a transparent and a well-documented IoT policy which should clearly define privacy-impacting procedures with clear implications even on policies outside certain geographical locations. Bandwidth consumption plays a vital role in IOT technology. Millions of sensors and actuators communicate over different servers that create data traffic which brings down the server. Also, most of the sensors currently communicate over an unencrypted link to communicate, leading to loopholes in security. Also as the number of devices increase, it will definitely put a strain on the spectrum of other wireless communications and critical power will come into question.

3.2 Performance Modeling and Capacity Planning

Capacity planning is mostly concerned with sizing the unpredictable fluctuations in IT resources Typically, IT Departments have a vague and generic understanding of their current resources and their usage pattern. It is mostly because of the convoluted environments involved, a number of people involved and also the fragmentation of responsibilities which makes capacity planning difficult.[3] Data about the resources may be prevalent, but are not recorded in a structured and systematic way. There are always uncertainties in analyzing current storage capacities which form one of the integral components in capacity planning and optimizing operational costs. Rough estimations on overall resource utilization and current capacity makes it a more laborious task since then everything has to be done from the scratch. Moreover, organizations often revert to performance modeling only in times of utter need which then brings about inefficient guesswork and too much urgency in the entire process.[10]

3.3 Cloud Computing

Enormous data acquisition that needs large processing speeds and storage resources on clouds can be viewed as one of the fundamental issues underlying cloud technology. With cloud technology coming into existence, there are obvious security allegations tagging along, but there is also a huge cost factor undermining possible solutions. The main problem with high security is that it comes with high costs. Implementing security solutions add on to prevailing cost for local hardware implementation. It also has the power to affect the response time of data transactions that are independent of the cloud infrastructure, yet slackening the system. Software licensing is yet another issue that software companies have to face. They have to make it mandatory for their clients to use software in a cloud environment and impose restrictions on the software that can run on computers which forced many cloud computing providers to rely on open source software in part since the licensing model for commercial software is not proving to be a good match to Utility Computing. However, there are different approaches that can be implemented to deal with such issues. Changing the license agreement and making it independent of the number of machines that uses, might turn out to be a good solution. Next, there are real authentication and authorization issues emerging from practically everywhere .The fact that sensitive or public cloud resources can be availed from everywhere on the internet tightens the need to identity of a user especially if users now range from employees, contractors, partners to customers. These issues then becomes of critical concern. The cloud customers investment in achieving certification that proves his compliance with industry regulations may be lost if the provider is not able to account for evidence of his own compliance with the relevant requirements. This again is an important issue that has to be taken care by the clients. It is mostly because of the data risks that a client is taking in sharing confidential data with a cloud provider.

4. Future Directions

As the concept of interconnecting devices generates enormous amounts of data, and if this transformation only takes a step forward, there are practical chances of data centres being literally flooded with overwhelming data that has to be synthesized, stored and analyzed, it will definitely push for the need for additional storage, network, and computing resources within short time. Also with enhanced levels of automation in almost every domain, there again will be a need to manage complex dynamic equipment for the long run. Following the obvious intuitions, everything here drives for a strong capacity management and performance modeling in internet of things and cloud technologies.[4]

References

[1] Internet of Things-White Paper, 1st ed. 2016.
[2] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Future generation computer system", 2016.
[3] White paper- CiRBA- eguide-capacity control
[4] Elsevier - special issues on IOT: Research challenges and solution
[5] Cyber Security and Internet of Things, 2016.
[6] White paper of Texas Instruments - The Evolution of Internet of things
[7] The ratrion, 2016.
[8] Capcity Planning decisions for data centres decisions-Whitepaper
[9] 2016[Online]. Available: http://wikipedia cyber security.
[10] X. Huang and S. C. Graves, "Capacity Planning in a General Supply Chain with Multiple Contract Types Single Period Model", 2016.

Author Profile

Bhautik Pipaliya is pursuing the B.Tech degree in Information and Communication Engineering from Institute of Engineering and Technology.

Devanshi Gariba is pursuing the B.Tech degree in Information and Communication Engineering from Institute of Engineering and Technology.