Cloud Computing: Security Issues and Research Challenges

Moulika Bollinadi
Under Graduate Student, MGIT, Hyderabad, Telangana, India.

Vijay Kumar Damera
Assistant Professor of IT, MGIT, Hyderabad, Telangana, India.

Abstract – Cloud Computing is a type of internet based computing which provides services via the internet and accesses the resources within the user enterprise either in a private-own-cloud or on a third-party server On Demand. The model is characterized by three attributes: scalability, pay-per-use, self-services. Many industries such as banking, healthcare, Retail, Education, Manufacturing and business are adopting this cloud technique due to efficiency of services provided by pay-per-use pattern which helps in accessing the networks, storage, servers, services and applications, without physically acquiring them [3]. The circumscribed control over the data may cause various security issues in cloud computing like Data crash, Misuse and reprehensible use of cloud computing, Insecure API, Wicked Insiders, Shared technology issues/multi-tendency nature, Account services and Traffic Hijacking. There are many new technologies, improvements and research proceedings happening every day in order to develop the security and to provide assurance for users [2]. This research paper brings a framework on what cloud computing is, main security risks and issues that are currently present in the field of cloud computing, research challenges, importance in key industries and also the personal hypothesis on future advances in the field of cloud security.

Index Terms – Security issues, Cloud Security, Cloud Architecture, Challenges, Automation of IT industry.

1. INTRODUCTION

Cloud Computing has become a compelling force in the world of Information Technology. It is considered as one of the key features for data storage, security, access, reliable nature on costs. Due to the advancement in technology, the usage of internet has been increased in a wide range and so the cost of the hardware and software too. In order to abate the cost of hardware and software by providing services when user demands over the internet, the cloud computing concept has been successful and gained a lot of popularity in a very little time period.

One main reason for the managements to move towards IT is not a new concept, it has recently become a paradigm of solutionsiscloudcomputing,astheyarerequiredtopaythe billings for the resources of only how much they consume. Though it distributed computing. In the year 1969 [4][5], L. Kleinrock predicted that, As of now, computer networks are still in their infancy. But as they grow up and become more sophisticated, we will probably see the spread of computer utilities which, like present electric and telephone utilities, wil lservice individual homes and offices across the country. We now observe, his anticipations were true and are indication of todays utility based computing paradigm. One of most gigantic changes in this world was happened in mid 1990s when grid computing came into existence and provided services on-demand.

Figure1: Overviewofcloudcomputing[1]

The term cloud computing was first influenced by Googles CEO Eric Schmidt in late 2006 [5][6]. From this we can understand that cloud is a new phenomenon formed by amalgamating the old ideas and concepts. Cloud is generally built on grid based architecture using the grid services and other technologies like virtualization and models. The main enabling technology of cloud computing is virtualization which separates physical computing devices into two or more virtual devices, so that it can easily manage the computing tasks. Cloud services are provided as major utility services like water, telephone, electricity using pay-as-you-use model. These services are generally described as XaaS where X can be anything like a Software or Infrastructure or platform etc. According to the past researches and results, in 2009 [7], the

availability of high-capacity networks, low-cost computers and devices as well as the widespread adoption of hardware Virtualization, Service-Oriented Architecture, Automatic and Utility computing led to a growth in Cloud Computing. In the year 2013 [7], it was observed that Cloud Computing had become a highly obtained service due to the advantages like High Computing Power, low service costs, scalability, high performance and accessibility.

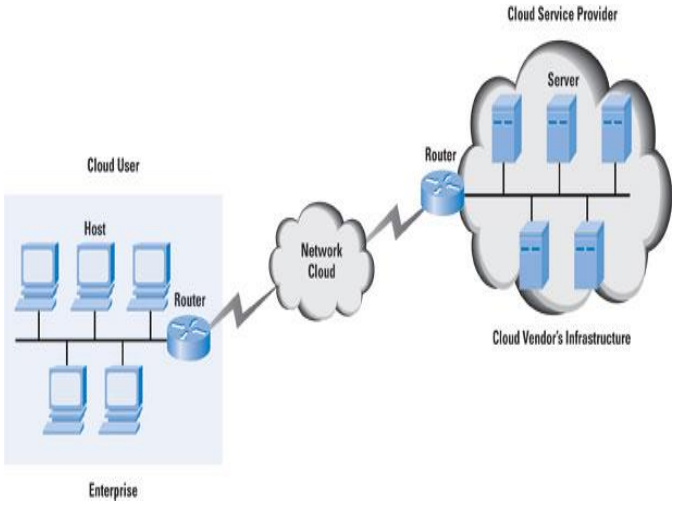

Figure2: ContextofCloudComputing[1]

2. ARCHITECTURE

The Cloud Computing generally contributes three types of services: [8]

2.1 Software as a service (S-a-a-S)

2.2 Infrastructure as a service (I-a-a-S)

2.3 Platform as a service (P-a-a-s).

2.1 Software as a service (S-a-a-S): S-a-a-S is also known as Cloud application Services which utilizes the web to deliver applications that are managed by third-party seller and whose interface is accessed on the customer side. Most S-a-a-S applications can be run directly from a web browser without any downloads or installation process, some require plugins. It is simple for S-a-a-S to keep up and bolster the endeavors since vendors deal with the works like applications, runtime, data, middleware, OSes, virtualization, servers, storage and networking.

The S-a-a-S has four common approaches: [9].

1. Single instance

2. Flex tenancy

3. Multi instance

4. Multitenant

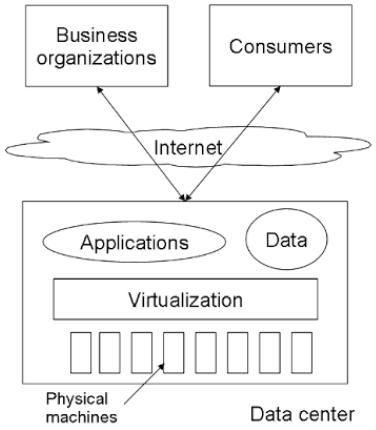

Figure3: Basic cloud computing Architecture [5].

Examples: Google Apps, Go-To Meeting, concur, Sales force workday, Citrix, WebEx, Cisco.

2.2 Infrastructure as a service (I-a-a-S): I-a-a-S, otherwise known as Cloud Infrastructure Services are models which perform tasks by themselves for accessing and monitoring which helps in incorporating the compute, storage, networking and networking services. Many I-a-a-S providers now offer databases, messaging queues, and other services above the virtualization layers. When compared to S-a-a-S and P-a-a-S, I-a-a-S clients are responsible for managing applications, data, runtime, middleware, and OSes.

Examples: Computer Compute Engine (GCE), Amazon web services (AWS), Cisco Meta-pod Microsoft Azure, Joynet.

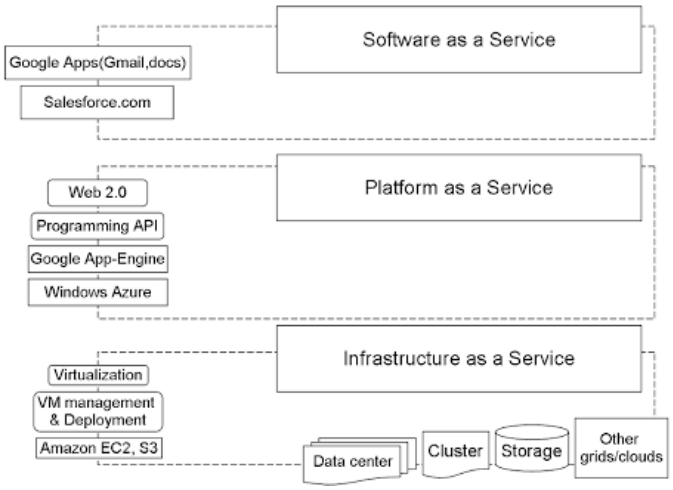

Figure4: Services provided by Cloud Computing [5].

2.3 Platform as a service (P-a-a-S): Cloud platform services, or P-a-a-S are generally used for application and other developments while providing cloud components to software. It makes the development, deployment of applications quick, testing, simple, and cost-effective. With P-a-a-S, enterprise

operations, or third-party provider, can manage many services like servers, O.Ses, virtualization, storage and networking.

Examples: Apprenda

3. IMPORTANCE OF CLOUD COMPUTING IN KEY INDUSTRIES

Cloud computing has become a major source for the industries. The survey conducted by the Economic Intelligence Unit gives a report that, over 90 percent of global enterprises use cloud computing as a part of industries. Cloud is the largest category in IT infrastructure budgets with over 33 dollar billion projected in 2015. Every industry has its unique technology dynamics. To understand the dynamics in cloud computing we must first understand the dynamics in key industries [3].

The following figure explains about the importance of Cloud Computing in five key industries namely Banking, Retail, Manufacturing, Education and Healthcare respectively.

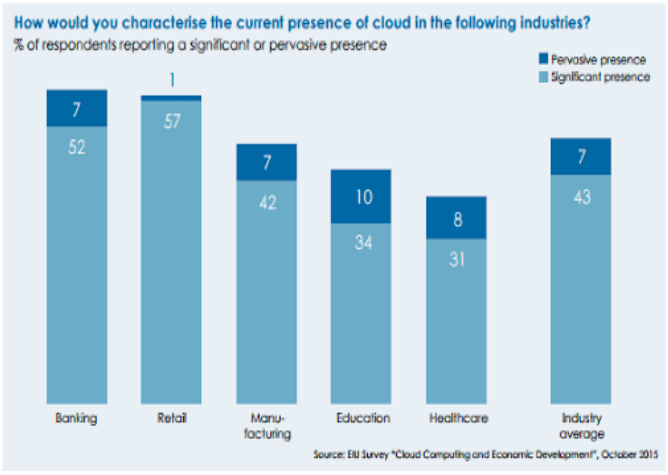

Figure 5: Characterizing the presence of cloud in the fivekeyindustriesin2015 [11].

If we observe in the graph of figure-5, the characterization in the present cloud computing is given by Pervasive presence and Significance presence. Pervasive means emphasizing the slightly different aspects in a single term which are ready to access and widespread deployment [10]. Significant presence is defined as significant differences in cloud adoption. The industries account a total average of 7 percent pervasive presence and 43 percent significant presence.

According to figure-6, Education, Financial Services and Business Services are the three industries which play the major role in the Cloud BI today.

Additional industries that have a relatively high level of interest in Cloud BI include retail and wholesale and telecommunications. Many Manufacturing challenges are creating new opportunities for advanced analytics.

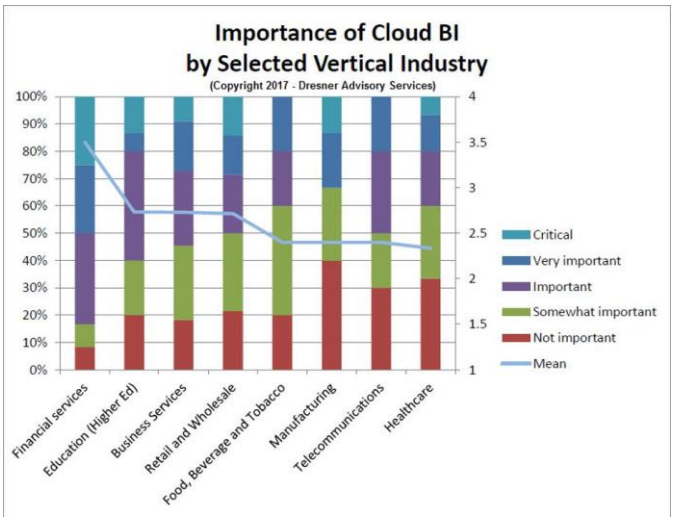

Figure 6: Importance of cloud BI in selected vertical industryin2017 [12].

3.1 Banking a distribution of legacy business:

There are two type of trends driving in cloud computing. First one is the adoption of cloud for bank-office and performing selected customer operations by traditional banking institutions. The second one is Fin-tech digital insurgents who are regularly using cloud-based services to compete in key banking products.

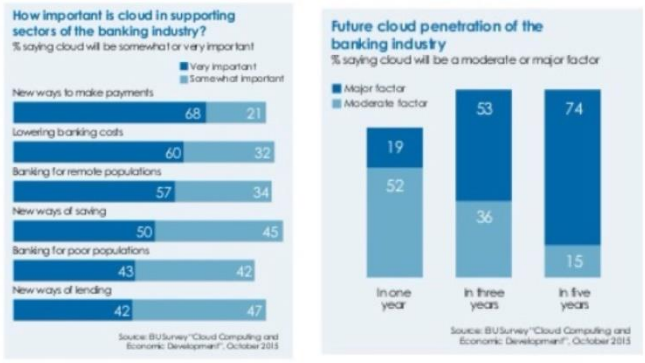

Figure 7: Future Cloud penetrations and Supporting sectors in banking industry [11].

According to EIU, these forces will gain a rapid rate of adoption of almost nine out of sixteen predict cloud which is, at present, in 2017 is one of the major factors in banking. The growth of cloud along with existing legacy systems, coupled with concerns about security.

The above figure-8 explains about the rapid growth of cloud computing in next three years. If we observe, it is estimated that in 2017, the average rate of growth of cloud computing is approximately one half of the rate of growth in 2020.

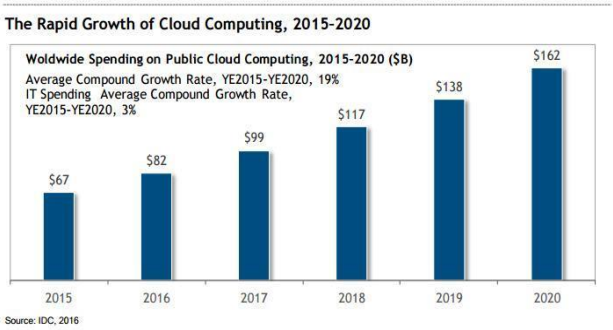

Figure 8: Rapid growth of cloud computing, 2015-2020 [22].

3.2 Retail- the growth of parallel business:

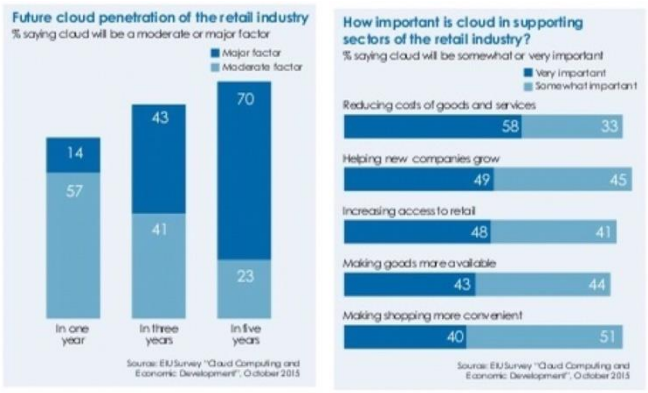

Figure 9: Cloud as major or moderate factor in Retail industry and importance in supporting sectors [11].

The retail experts predict that the cloud will be the major or moderate factor for Retail industry in the future years. The 2015 report (shown in figure-9) explains that within five years there is going to be a five-fold increase as a major factor retailing.

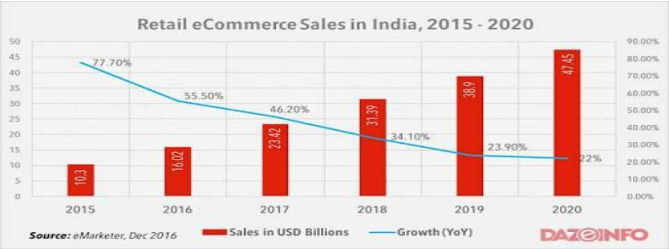

Figure 10: Retail e-Commerce sales in India, 2015-2020 [20]

By lowering the prices and reducing the costs of the consumer, the cloud appears to make retailing more user-friendly due to the increase in access of technology. The increase in growth of new business and new products indicates the clouds place as the central technology of e-commerce

We can observe from figure-10 that the estimated that between 2016 and 2020, retail e-Commerce sales in India is going to be increased by 3x, reaching $47.45 billion. The retail e-Commerce industry in India is expected to account a required amount of share among total retail sales.

3.3 Manufacturing- a special case of cloud adoption in industries:

Manufacturing has become the leading driver of the economic growth. According to EIU, in 2015, manufacturing accounts almost one eighth of employees around the globe and accounts up to 16 percent of global GNP. It is responsible for 20 percent of global innovation and funds 77 percent of global research and development.

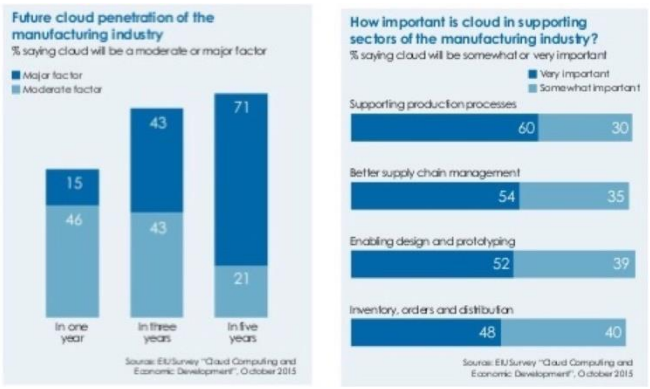

Figure 11: Cloud Major or moderate factor in Manufacturing industry and importance of Cloud in Manufacture industry. [11]

Not to be surprised manufacturing accounts 3 percent of global productivity. These all factors will therefore focus on the impact of cloud on the key manufacturing sector. Despite this, Cloud has a larger impact on digital manufacturing. When coupled with radio-frequency identification (RFID), the cloud enables inbound parts to be tracked around the globe.

But this effect goes beyond tracking parts and provides us appropriate services like

(i) Cloud and manufacturing supply chain:

1. Reduction in supply chain costs.

2. Cloud can connect, expand and diffuse the global base of suppliers.

3. Cloud supports partnership between customers and suppliers.

(ii) Cloud and design prototyping:

1. Reducing costs.

2. Accelerating time to market.

3. Increasing customization of manufacturing products.

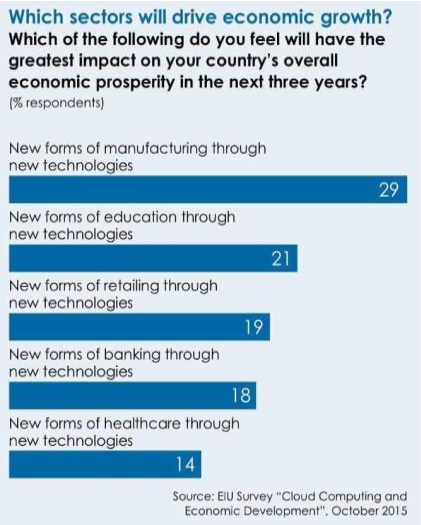

Figure 12: Greatest impact on country's overall economic prosperity [11].

(iii) Cloud and the production process:

1. Cost reduction through operating efficiencies.

2. Boosting manufacturing flexibility.

3. Greener manufacturing.

(iv)Cloud and manufacturing customer: The traditional manufacturer-customer relationship can be expressed in two steps:

1. A product is sold to the customer.

2. The supplier disappears until a new product is sold.

The result for these is that the manufacturer is no longer a supplier, but has become an energy manager for the building, instead of selling the product. This collaborative cloud enabled relationship can be found in customer wearable, building controls or air turbines.

3.4 Cloud technology and education:

The development of cloud in the field of education is slower when compared to the other industries. The reasons for this slower rate include less competitive environment and slower rates of adopting the technology.

After much initial stages, online education has suffered many disappointments as MOOCs (massive open online courses). It is also known that due to the lack of knowledge large number of enrolled students did not pursue their studies.

The adoption speed took a minimum span of 3 years and at present in 2017 cloud looks set to impact the entire spectrum of education.

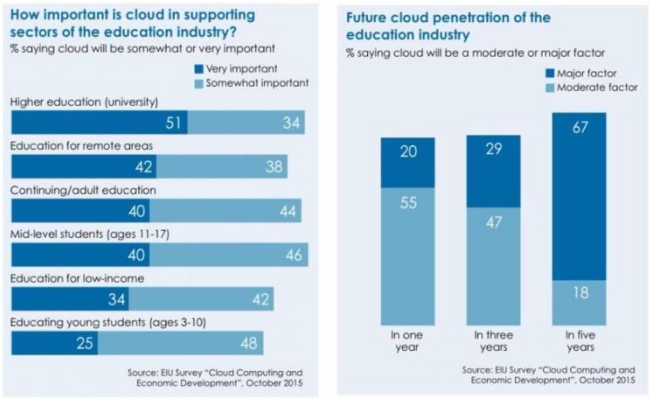

Figure 13: Importance of cloud in supporting sectors and cloud as major or moderate sector [11].

3.5 Cloud and healthcare changing the relationship between doctor and a patient:

The one field where cloud has an impact in research is in healthcare and a doctor-patient relationship.

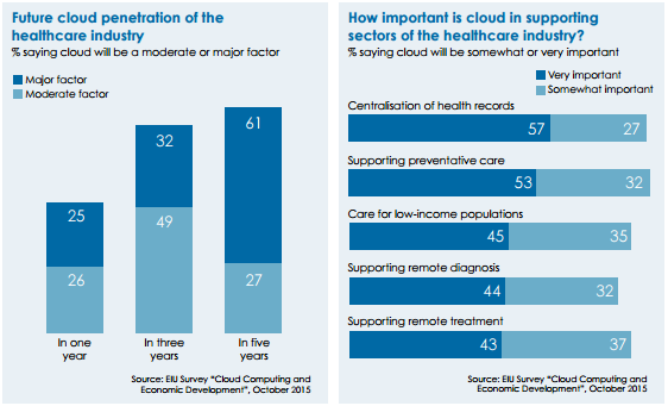

Figure 14: Cloud has major or moderate factor in the field of healthcare and importance of cloud in supporting sectors [11].

Remote diagnosis and treatment are used to enhance the knowledge of their own situation a reconsidered as main support in field of healthcare. It may also help in increasing the knowledge on usage of medicine and avoiding the harmful situations supporting the industry for a long time.

4. APPLICATIONS

The applications of cloud computing are as follows [19]:

1. It provides secure data storage center.

2. Cloud Computing systems reduce the need for advance hardware on users which is also responsible for reducing the hardware costs.

3. Cloud Computing can be realized by sharing between different equipment.

4. The Cloud provides approximately infinite possibility of use of internet for users.

5. SECURITY ISSUES IN CLOUD COMPUTING

There are various security issues for cloud computing as it comprises of numerous advancements including systems, databases, working frameworks, virtualization, asset planning, exchange administration, stack adjusting, simultaneousness control and memory administration. Similarly, security issues for greater number of these frameworks and technology are pertinent to Cloud computing.

According to the RSA conference which was conducted in the March 2016, the CSA (Cloud Security Alliance) has released the list known as Treacherous 12, which includes the top 12 Cloud Computing threats in 2016. The following are the 12 threats in cloud computing [13].

5.1 Data Breaches

5.2 Compromised credentials and broken authentication

5.3 Hacked Interfaces and APIs

5.4 Exploited system vulnerabilities

5.5 Account Hijacking

5.6 Malicious Insiders

5.7 The APT parasite

5.8 Permanent data loss

5.9 Inadequate diligence

5.10 Cloud services abuses

5.11 Dos attacks

5.12 Share technology and Share dangers

5. 1 Data Breaches:

Due to the improved technology, large amount of data is stored in cloud servers, which becomes a target for the hackers. More the amount of data exposed, greater will be the damage to the society and users. The exposure of personal profile would be a normal one, but breaches which involve health information, trading secrets, intellectual property rights would bring a larger destruction. Though Cloud provider typically disposed security controls to protect their environments, it is enterprises which are responsible for securing their own data in cloud. Use of multi-factor authentication and encoding the data or information so that only authorized users can access it.

5.2 Compromised credential sand broken authentication:

Data breaches and other attacks frequently result from slack authentications, weak passwords, poor key or certificate management. Sometimes, not only organizations even we forget to remove the access after our job is done. We can consider for example, the Gmail account if we login in the public accessing places (internet cafes) and forget to logout after our use, exposes our own private data to others. It is our responsibility to remember everything and take care. To avoid these issues, Multi-factor authentications such as one-time passwords, phone-based authentications, OTPs, security questions would make the attacker harder to login from stolen passwords. The rotation of cryptographic keys periodically will not only keep the records secure but also make the resources difficult for the attackers who use keys without authorization.

5.3 Hacked Interfaces and APIs:

At present, every cloud service provides APIs. They are used to manage the cloud services, management, orchestration, monitoring. The interfaces and APIs which are weak would expose the authorizations to security issues like confidentiality, integrity, availability and accountability. It is recommended by CSA, to focus on threat modeling applications such as architecture/ design which are the primary concepts for the future developments and also to examine the flaws in the security-coding reviews and high level of testing.

5.4 Exploited system vulnerabilities:

We have been facing the problem of bugs since a very longtime. One can say that they are always observed in one or the form. As the usage of technology has increased in a wide range, these vulnerabilities had become a bigger issue. The sharing of memory, data bases and other data among the organizations would lead to data crash or reports larger bugs and later on even may be affected by virus too. To eschew these bugs and system vulnerabilities one may probably have to scan the systems, mobile phones etc. regularly and try to find the solutions for the reported bugs.

5.5 Account Hijacking:

Figure15: Security concerns with cloud computing [14].

One of the most common and daily heard issues in the society at present is account hijacking. There may be various reasons

for hijacking such as sharing our credentials to others, sharing of our data to third-party vendors during online transactions and so-on. The attackers who would hijack our account may probably even manipulate the data, change the transaction details, even use the other cloud applications connected to the account to cause further attacks. The only thing we can do at present is to be careful while sharing our credentials and to always keep a follow up whenever the things go wrong and report them immediately.

5.6 Malicious Insiders:

These threats generally are appeared from the people who work in the organizations as employees, business associates and have the valuable information regarding the organizations which are to be maintained securely and secretly. By limiting the accessing needs in the computer systems during working hours and by encrypting the routine job such as malicious we can avoid these insider threats to certain extent [15]. Any sensitive information regarding the users if accidently is provided in the servers will surely affect their reputation and business for many years. Thus, proper training is also necessary for the people who are going to manage those sectors without complicating the things further.

5.7 The APT parasite:

The APT is a continuous hacking process, synthesized by a person or group of persons targeting a specific organization [16]. It is well known for attacking private organizations for business motives. This advance process uses a malware to cause vulnerabilities (virus, bugs, installations) in the system. Consider an example, The Stuxnet computer worm, which attacked the Computer hardware of Iran's nuclear program [18]. The Iranian government considered this to be an APT because it used a malware program code which spreads itself to all the computers using a computer Network depending upon the security failures. In the recent years, the threats include direct attacks, USB drives preloaded with malware coding.

5.8 Permanent Data loss:

5.9 Inadequate diligence:

Associations that grasp the cloud without completely understanding nature and its related dangers may experience a horde of business, money related, specialized, legitimate, and consistence chances. Due to constancy applied, whether the association is attempting to relocate to the cloud or combining (or working) with another organization in the cloud. For instance, associations that neglect to investigate an agreement may not know about the supplier's obligation if there should be an occurrence of information misfortune or rupture. Operational and building issues emerge if an organization's improvement group needs nature with cloud advancements as applications are sent to a specific cloud.

5.10 Cloud service abuses:

In 2013 [17], cloud abuse was considered as one of the top most threats and is still continuing. The main concept of cloud service abuse is that the hackers use the social media services to understand and extract different codes so, that they can disturb the cloud environment. Once this occurs, the organizations may face the problems like shut down of computers, erase of the necessary data. To avoid this issue we must keep a track on identifying the assets, Analyzing critical information, Analyzing the threats and vulnerabilities, risks while accessing and finally fix the problem with safeguard defense layers.

5.11 DOS attacks:

They critically affect the performance of the system. The system may run out of time and even becomes lower than the normal condition. The DOS attacks consume more power due to which our billing expenses also increases. The clue for this is, anticipating the threats before itself and access to the necessary resources.

5.12 Shared Technology and Shared Dangers:

Cloud service provides share infrastructure, platforms and applications. If a bug arises in any of the mentioned layers, it affects the secured data which directly affects the users. A defense-in-depth technique is suggested by CSA including the multi-factor authentication on all hosts, host based and network based systems.

6. RESEARCH CHALLENGES IN CLOUD COMPUTING

Although cloud computing has quickly come into the existence. The researches of cloud computing are still in an early stage. Many issues have not been resolved and new challenges have been emerging in every industry day-by-day. The following are few research challenges in cloud computing.

6.1 Service level agreement (SLA)

6.2 Cloud data management and security

6.3 Data Encryption

6.4 Virtual machines migration

6.5 Access controls

6.6 Multi-tenancy

6.7 Reliability and availability of services.

6.1 Service level agreement (SLA):

If needed, several instances of one application are replicated on multiple servers on priority basis. Most of the vendors create SLAs to make a protective shield against the legal issues, offering minimum assurance to other users. Few important issues like Data protection, outages and price structures are

necessary to be considered before signing the contract with the organizations [2]. Some of the all- time questions regarding SLAs are as follows: Are the services provided going to be 99.9 percent safe? Will there be problems like sharing of our private data during the low servers and breakdowns? Are they going to keep our data? if yes, then where and how long? Can we get an assurance that our data will be safe with them without any misuse? Is there any SLA that is associating with backup, achieve and preservation of our data? There is a lot of scope and research to do on SLA sand is surely an important research area in cloud computing.

6.2 Cloud data management and security:

Cloud data concept is an important research topic in cloud computing. Cloud data can be a large data, unstructured or typically structured with rare cloud updates. The infrastructure provider, in this context, must achieve the objectives like confidentiality, auditability. Confidentiality is for secure data access while transfer and auditability are for checking whether the arrangement of applications has been altered or not. Cryptographic protocols are used to achieve the Confidentiality, whereas auditability can be achieved using remote attestation techniques. The file systems such as GSF and HDSF are different from traditional distributed file systems especially in their storage structure, access pattern and application programming interface. Due to this, there may be compatibility issues with long-lasting file, systems and applications. Several research efforts have studied this problem.

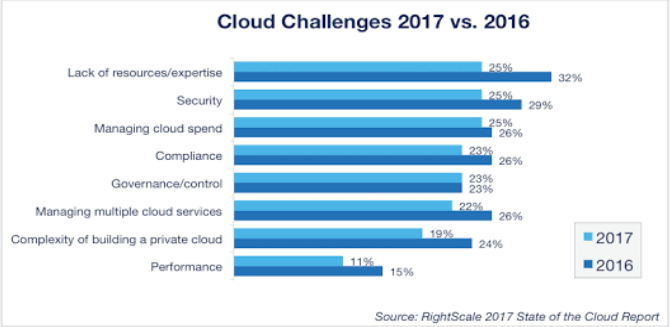

Figure16: CloudChallenges2017vs. 2016 [21]

6.3 Data Encryption:

It is a key technology for data security. We have to remember that security can range from similar, medium or high (whether in cost, issue). We can consider APIs as an example here. When an object arrives at the cloud, due to the data gets decrypted and stored. The questions like are there any options to encrypt the data before storing it? Is there any possibility to understand our cloud computing and take the required measures for making it secure? These type of questions are still not yet understood and gained a clear knowledge in cloud computing and are needed to be resolved.

6.4 Virtual machine migrations:

To balance the load across the data center, virtual machine migration can be enabled in cloud computing. It is evolved from techniques of process migration. In 2011, Xen and VMW are have implemented live migration of VMs that involves extremely short down times ranging from tens of milliseconds to a second. The major benefits like avoiding hotspots; however, has not been implemented straightly. Detection of work load hot spots and initiating a migration lacks and the time taken to respond to sudden workload changes has been implemented.

6.5 Access Controls:

The identity and authentication are very important in managing the security. The control of these access managements would help us to build the security of the users but also give us some research challenges like How to improve the security? How well is the password strength and change frequency does the provider assure us? What are the recovery methodologies that should be implemented when the password and username are corrupted? How are logs and messages secured without displaying? How are the changed passwords delivered to the users? All these are not different or new things. But we still have to do a lot of improvements and gain knowledge, so that, we can introduce new security measures which brings more clarity and assurance to the future scope.

6.6 Multi-tenancy:

The unique nature about Multi-Tenancy in Cloud Computing is that both the attacker and the victim share the same server (i.e. physical machine (PM)). Such a setup cannot be mitigated by traditional security techniques and measures because it is not designed to penetrate inside servers and the monitoring techniques are limited to the network layer. From the past researches we have found that there is no way to eliminate the Multi-Tenancy effect as it provides us key benefits. But the effect could be minimized by obtaining a smart resource allocation technique. In other words, a resource allocation technique will increase the level of difficulty of achieving Multi-Tenancy for customers but can be easily managed by Cloud providers. What is interesting of Multi-Tenancy is that in order to achieve it for targeted victims, the attack needs to invest a lot of effort, time and cost. So, by making Multi-Tenancy difficult to be achieved by customers, we are restricting the number of potential attackers. The proposed technique to challenge for this is threat model and attack model which bring the advancements and increase the efficiency of multi-tenancy.

6.7 Reliability and availability of services:

The concept of reliability comes into the presence when the cloud provider delivers on-demand services. The users mainly depend upon the network services (availability of network in

slow signal stages) when it comes to reliability and availability. One good example for this is Apple's Mobile Me cloud service, which stores and synchronizes data across multiple devices. It was initially not an up-to the mark output as many users were not able to synchronize the data correctly. In order to get over such problematic circumstances, providers had turned themselves to technologies such as Google Gears, Curl, and Adobe AIR which allow cloud based applications to run with local time, sometimes even accept to run in the absence of a network connection. On Considering the usage and implementation of software such as 3D gaming applications and video conferencing systems, reliability has progressed up to a certain extent in the past five years but is still challenge to achieve for an IT solution that is based on cloud computing.

7. FUTURE ADVANCES IN THE FIELD OF CLOUD COMPUTING

Down the line of five years, the whole IT industry is moving towards the concept known as Automation. Probably in the next five years, Artificial Intelligence (AI) and Machine Learning (ML) are going to play a major role in the Automation process. As the development of automation increases, we can expect the decrease in the traditional programming jobs in IT industry.

In support to the mentioned context, let's assume an example. In the process of automation, when a machine takes the control of building the logic instead of human brain, we can imagine the damage going to be caused in terms INTRUSION. If a traditional programmer is aiming to exploit the computer resources with the help of his/her skills and abilities, it takes a descent amount of time to perform (or) execute the given assignment. But if a machine performs the same thing with the help of technology we have today and the intelligence it got from machine learning, it takes fraction of seconds to do the assignment. In this scenario, the traditional IDS systems would no more be suitable in the context of automation. So, there is an immediate need in strengthening the traditional security mechanisms in terms of FIRE WALLS and IDS.

According to the report, Cyber Security: Threats, Reports and Challenges [23], in 2016, only one percent of the world's total devices are using the internet and cloud based services. It is estimated that by 2023, 85 percent of the world's devices and industries are going to opt the internet and cloud as the main source of service. By this we can understand that, as the usage of number of IOT devices increases, load on the cloud also increases. This also results in the increase of security issues which can't be solved by using methods that are implemented at the present. We require the advancements in maintaining security and new researches must be carried out on How to increase the cloud security? How to make our security system strong? So that everything will be in our control even if an attacker tries to hack the systems or services by using new technologies in the automation process.

8. CONCLUSION

Cloud Computing is an emerging technology with a concept of distributed computing. Though it has not come into a full force at present, the future of the software industry is completely going to be dependent on this concept. In this paper, we first discussed about what cloud computing is and Different services provided by Cloud. Later, Importance of cloud computing in key industries, Security issues and research challenges, Applications of cloud computing and future advancements in cloud computing technology. We have observed that here are several security challenges including security aspects of network and virtualization. This paper has highlighted all the security issues in cloud computing and possibly how to avoid them too. New security technologies must be developed and older technologies are needed to be radically tweaked to be able to work with cloud architecture. We believe that Industries are the main sectors for usage of cloud services. The cloud usage in five key industries are studied in this report along with the increase in cloud usage from 2015 to 2017. Last but not least, as whole IT industry is looking forward for the process of Automation, we have provided an overview of how it is going to be with our imagination and what are the basic security issues that are going to be faced in the future. As Automation in Cloud Computing is still an ideal process which needs more clarity and research to be done, we hope that our work will provide a better understanding of design challenges in cloud computing and pave the path for future research in this area.

REFERENCES

[1] G. O Rabi Prasad, Manas Ranjan, Suresh Chandras Cloud "Computing: security issues and Research Challenges" published in IRACST-International Journal of Computer Science and Information Technology and Security (IJCSITS), Vol. 1, No. 2, December 2011.

[2] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I and Zaharia M, "A view of cloud computing, Communications" of the ACM Magazine , 2010, 53 50-58.

[3] Ashraf I, "An over view of service model of cloud computing" published in Int. J. of Multidisciplinary and Current Research, vol.2, 2014, 779-783.

[4] Bala Narayada Reddy G," Cloud computing-types of cloud," 2013, Retrieved from http://bigdatariding.blogspot.my/2013/10/cloud-computingtypes-of-cloud.html.

[5] Christina A A, "Proactive measures on account hijacking in cloud computing network" published in Asian Journal of Computer Science and Technology, vol.4, 2015, 31-34.

[6] Choubey R, Dubey R and Bhattacharjee J, "A survey on cloud computing security challenges and threats" published in International Journal on Computer Science and Engineering (IJCSE), vol.3, 2011, 1227-1231.

[7] Leonard Kleinrock, "An internet vision: the invisible global infrastructure" published in Ad Hoc Networks, 11, 2003, 1(1):3.

[8] Dinesha H A and Agrawal V K, "Multi-level authentication technique for accessing cloud services" published in International Journal on Cloud Computing: Services and Architecture (IJCCSA), vol.2, 2012, 31-39.

[9] Doelitzscher F, Sulistio A, Reich C, Kuijs H and Wolf D, "Private cloud for collaboration and e-Learning services: from I-a-a-S to S-a-a-S" published in J. Computing-Cloud Computing, 2011, 91 23-42.

[10] Hamlen K, Kantarcioglu M, Khan L and Thurai singham B, "Security issues for cloud computing Optimizing Information Security and Advancing Privacy Assurance: New Technologies" published in International Engineering Research and Innovation

Symposium (IRIS), IOP Publishing, IOP Conf. Series: Materials Science and Engineering ,160, 012106, vol.8, 2016, 150-162. doi:10.1088/1757-899X/160/1/012106

[11] Jain S, Kumar R, Kumawat S and Jangir S K, "An analysis of security and privacy issues, Challenges with possible solution in cloud computing", Proc. of the National Conf. on Computational and Mathematical Sciences (COMPUTATIAIV), 2014, 1-7.

[12] Kandias M, Virvilis N and Gritzalis D, "The insider threat in cloud computing" Proc. of 6th International Conf. on Critical Infrastructure Security, 2011, 95-106.

[13] Khoshkholghi M A, Abdullah A, Latip R, Subramaniam S and Othman M, "Disaster Recovery in Cloud Computing: A Survey Computer and Information Science," vol.7, 2014, 39-54.

[14] Khurana Sand Verma A G, "Comparisons of cloud computing service model: S-a-a-S, P-a-a-S, I-a-a-S," published in International Journal of Electronics and Communication Technology (IJECT), vol.4, 2013, 2932.

[15] Kiblin T, "How to use cloud computing for disaster recovery," 2011, Retrieved from http://www.crn.com/blogs-oped/channel-voices/230700011/how-to-use-cloud-computingfor-disaster-recovery.htm.

[16] Kill A, "Cloud computing risk: Due diligence and insurance," 2013, Retrieved from http://www.metrocorpcounsel.com/articles/17928/cloudcomputing-risks-due-diligence-and-insurance.

[17] King N J and Raja V T, "Protecting the privacy and security of sensitive customer data in the cloud Computer law and Security Review," vol.28, 2012, 308-319.

[18] Kuyoro S O, Ibikunie Fand Awodele O, "Cloud computing security issues and challenges" published in International Journal of Computer Networks (IJCN), vol.3, 2011, 247-255.

[19] LiA, Yang X, Kandula Sand Zhang M, "Cloud Cmp: Comparing public cloud providers" Proc. of the 10th ACM SIGCOMM Conf. on Internet measurements, 2010, 1-14.

[20] Ramanathan S, Goel S and Alagumalai S, "Comparison of cloud database: Amazon's Simple DB and Google's Big table" published in International Journal of Computer Science, Issues 8, vol.2, 2011, 243-246.

[21] Rocha F and Correia M, "Lucy in the sky without diamonds: Stealing confidential data in the cloud" Proc. of the 1st Int. Workshop on Dependability of Clouds Data Centers and Virtual Computing Environments (DCDV), 2011, 1-6.

[22] Sekhar R V, Nandini N, Bhanumathy D and Hemalatha M, "Identity based authentication for data stored in cloud" published in International Journal of Advanced Research in Computer Science and Software Engineering, vol.5, 2015, 243-247.

[23] Cyber Security: Threats, reports and challenges.