EasyChair Preprint

№ 10526

Research Paper(Analysis & Review on Security Challenges and Issues on Cloud Computing)

Amlesh Kumar, Ravi Pratap Singh and Sourabh Kumar

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

July 9, 2023

ANALYSIS AND REVIEW OF SECURITY CHALLENGES AND ISSUES ON CLOUD COMPUTING

Amlesh Kumar – 22SCSE2030512
Sourabh Pratap – 22SCSE2030485
Ravi Pratap Singh – 22SCSE2030170

ABSTRACT- Cloud computing has emerged as a dominant paradigm for delivering various services and storing data remotely. However, the widespread adoption of cloud computing also raises significant security concerns and poses research challenges. This research paper explores the security issues associated with cloud computing and identifies key research challenges that need to be addressed to ensure the confidentiality, integrity of data in cloud environments.

Security Issues:

Data Privacy: The migration of sensitive data to the cloud raises concerns about unauthorized access and privacy violations. Ensuring data privacy is crucial to protect sensitive information from unauthorized disclosure.

Data Integrity:

Maintaining the integrity of data stored in the cloud is essential to prevent unauthorized modifications, tampering, or corruption. Techniques such as cryptographic mechanisms and data validation techniques are needed to ensure data integrity.

Data Loss and Recovery:

Cloud service providers can experience data loss due to hardware failures, outages, or natural disasters. Efficient data backup, disaster recovery, and fault tolerance mechanisms are necessary to mitigate the risk of data loss and facilitate quick recovery.

Multi-tenancy and Virtualization:

Cloud environments often involve the sharing of physical resources among multiple tenants. The challenge lies in ensuring adequate isolation and security between different tenants to prevent unauthorized access or data leakage.

Insider Threats:

Trusted insiders, including cloud administrators and employees, can misuse their privileges to access or manipulate sensitive data. Detecting and mitigating insider threats is critical to maintaining the security of cloud environments.

Research Challenges:

Access Control and Authentication: Developing robust access control mechanisms and authentication protocols to ensure that only authorized users and entities can access cloud resources.

Secure Data Sharing:

Enabling secure and controlled data sharing among multiple users or organizations in a cloud environment while preserving data confidentiality and integrity.

Intrusion Detection and Prevention:

Developing advanced detection and prevention systems to identify and respond to malicious activities or attacks targeting cloud infrastructures.

Secure Virtualization:

Enhancing the security of virtualization technologies used in cloud computing to prevent unauthorized access and ensure isolation between virtual machines and tenants.

Trust Management:

Developing trust models and mechanisms to assess the trustworthiness of cloud service providers and enable users to make informed decisions when selecting and utilizing cloud services.

Addressing these security issues and research challenges is crucial for the widespread adoption of cloud computing and the realization of its full potential while maintaining data security and privacy.

INTRODUCTION

The world of information technology is now dominated by cloud computing. It is regarded as one of the essential characteristics for cost-effective data storage, security, access, and reliability. The use of the internet has grown significantly as a result of technological advancements, as has the price of hardware and software. The cloud computing concept has been effective and garnered a lot of popularity in a very short time period. It does this by offering services when user desires over the internet in order to reduce the cost of hardware and software.

One main reason for the managements to move towards IT is not a new concept, it has recently become a paradigm of solutions is cloud computing, as they are required to pay the billings for the resources of only how much they consume. Though it distributed computing. Real world estimates of average server used in data centres range from 5% to 20%. This may sound shockingly low, but it is consistent with the observation that for many services the peak workload beat the average by factors of 2 to 10.[1] 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.

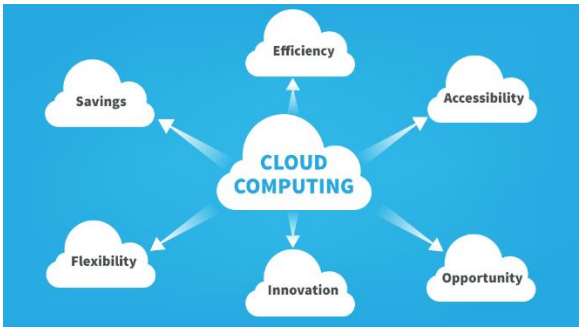


Figure1: Overview of cloud computing

Eric Schmidt, CEO of Google, was the person who first popularized the phrase cloud computing in late 2006. From this, we might infer that clouds are a brand-new phenomena created by fusing together previous notions and theories. The majority of cloud architectures use grid services, along with other technologies like virtualization and modelling. The primary technology for cloud computing is virtualization, which divides actual computing hardware into two or more virtual devices so that it can manage the computing chores with ease. With a pay-per-use business model, major utilities like power, water, and cloud services are offered. The primary technology for cloud computing is virtualization, which divides actual computing hardware into two or more virtual devices so that it can manage the computing chores with ease. With a pay-per-use business model, major utilities like power, water, and cloud services are offered. These services are typically referred to as XaaS, where X can stand for anything, including software, infrastructure, platforms, etc. In 2009, the availability of high-capacity networks, inexpensive computers and gadgets, as well as the broad adoption of hardware virtualization, service-oriented architecture, automatic and utility computing, contributed to an increase in cloud computing, per previous studies and findings. Due to benefits including high computing power, low service prices, scalability, high performance, and accessibility, cloud computing was found to have become a highly sought-after service in 2013.

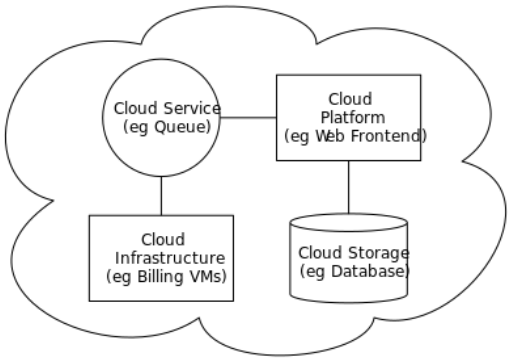


Figure2: Context of Cloud Computing

ARCHITECTURE

The Cloud Computing generally contributes three types of services:
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).

S-a-a-S (software as a service)S-a-a- S, or cloud application services, uses the internet to deliver applications that are controlled by third parties and whose user interfaces are accessed by customers. The majority of SaaS programs may be used straight from a web browser without downloading anything or requiring installation, while some do need plugins. Since suppliers handle tasks including apps, runtime, data, middleware, OSes, virtualization, servers, storage, and networking, S-a-a-S can easily maintain and support the initiatives.

The S-a-a-S has four common approaches:

1.Single instance

2.Flex tenancy

3.Multi instance

4.Multitenant

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

IaaS (infrastructure as a service): I-a-a-S, or cloud infrastructure services, are models that carry out access and monitoring duties on their own and aid in incorporating computation, storage, networking, and networking services. Databases, messaging queues, and other services are now widely available from IaaS providers above the virtualization layers. In contrast to S-a-a-S and P-a-a-S, I-a-a-S clients are in charge of managing OSes, runtime, middleware, and applications.

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

Platform as a Service (PaaS): PaaS, or cloud platform services, are typically used for software development while supplying cloud components to applications. It facilitates rapid application creation, deployment, testing, simplicity, and cost-efficiency. P-a-a-S allows business operations or third parties to handle a variety of services, including servers, operating systems, virtualization, storage, and networking.

Examples: Apprenda

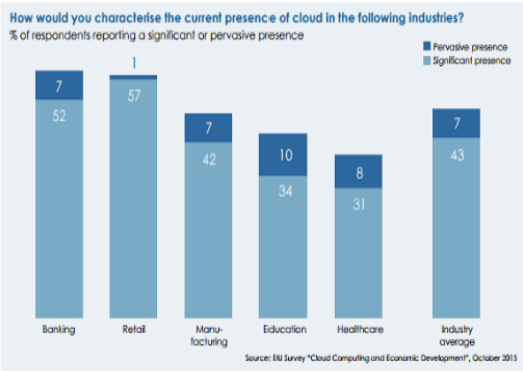


Figure3: Characterizing the presence of cloud

IMPORTANCE OF IN THE INDUSTRIES

The industries now rely heavily on cloud computing. According to the Economic Intelligence Unit survey, more than 90% of international businesses use cloud computing in some capacity. With approximately $33 billion expected for IT infrastructure in 2015, cloud is the largest budgetary category. Every sector has its own distinct technology dynamics. We must first comprehend the dynamics in important businesses in order to understand the dynamics in cloud computing.

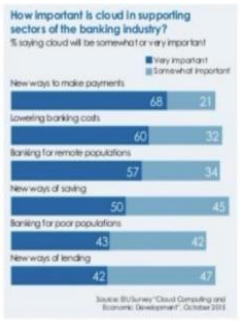
The retail and wholesale sectors as well as the telecoms sector are other sectors with a fair amount of interest in cloud business intelligence. The need for advanced analytics is growing as a result of numerous manufacturing difficulties. The retail and wholesale sectors as well as the telecoms sector are other sectors with a fair amount of interest in cloud business intelligence. The need for advanced analytics is growing as a result of numerous manufacturing difficulties.

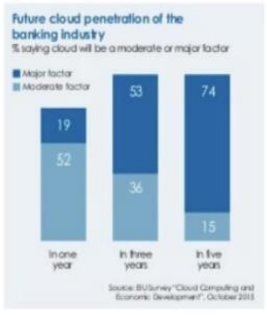
Banking a distribution of legacy business:

Two trends in particular are influencing cloud computing. The first is traditional banking institutions using the cloud for their bank offices and a select few customer operations. The second is digital rebels in the financial technology space who often use cloud-based services to compete in important banking-products.

The cloud, which is currently one of the key aspects in banking, will be adopted at a rate of approximately nine out of every sixteen people, according to EIU. the expansion of cloud computing, legacy systems already in place, and security worries.

The accompanying demonstrates how cloud





computing will expand quickly over the next three years. If we see, it is predicted that the average growth rate of cloud computing would be almost half that of 2020 in 2022.[5]

Retail- the growth of parallel business:

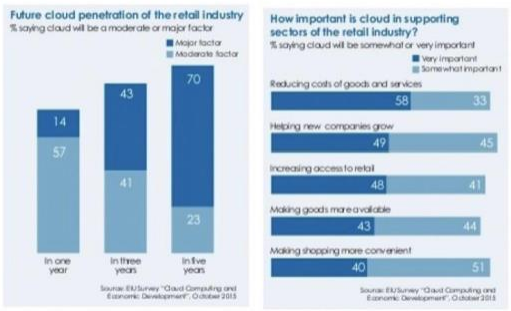


Figure:5: Cloud as major or moderate factor in Retail industry and importance in supporting sectors

The cloud will likely play a significant or moderate role in the future of the retail sector, according to industry analysts. The 2015 research (shown in figure 9) states that a five-fold rise will be a significant factor in retailing within five years.

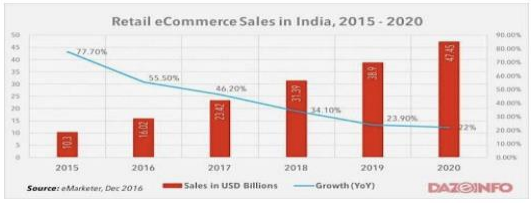


Figure:6: Retail e-Commerce sales in India

Because more people have access to technology, it appears that the cloud makes retailing more user-friendly by lowering costs for consumers and lowering prices. Increased new company and product development implies that cloud computing is now the primary e-commerce technology.

It is hardly surprising that manufacturing represents 3% of global productivity. As a result, all of these elements will concentrate on how the cloud will affect the important industrial sector. Cloud, however, has a greater effect on digital manufacturing. The cloud makes it possible to trace incoming parts all over the world when used in conjunction with radio-frequency identification (RFID).

However, its impact goes beyond identifying components and offers us useful services such

Cloud and manufacturing supply chain:

Reduction in supply chain costs.

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

Cloud supports partnership between customers and suppliers.

Cloud and design prototyping:

Reducing costs.

Accelerating time to market.

Increasing customization of manufacturing products.

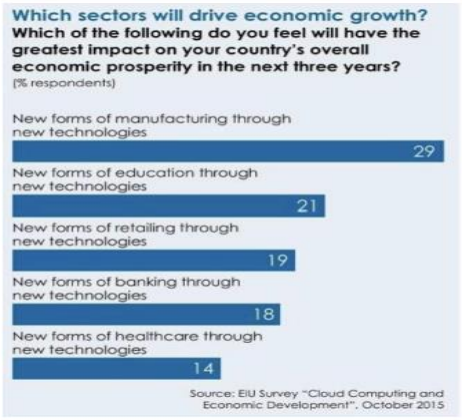


Figure:7: Greatest impact on country's overall economic prosperity

Cloud and the production process:

Cost reduction through operating efficiencies.

Boosting manufacturing flexibility.

Greener manufacturing.

Cloud and manufacturing customer:

The manufacturer-customer relationship can be defined in various steps:

A product is sold to the buyer.

The supplier not appear until a new product is sold.

The result of above both condition manufacturer no longer supplier and become an energetic manager for building blocks instead of selling the product.

Cloud technology and education:

Compare with other sectors, the development of cloud computing is rarely slowed in educational sectors. There are less intense competition and more gradual adoption is the factors of this slow rate.

MOOCs (massive open online courses) is the experienced setbacks which is numerous in online

educations in various phases. Additionally many of the students are report the lack of understandings in online educations. In the field of online healthcare and diagnosis therapy which are operate remotely, used to improved patient's health. Although it might be some contributions in order to understanding of how to prevent drug and what is the use of that particular drugs, which is the benefits of the drug in emergency situations.

APPLICATIONS

There are some following applications of cloud computing:

1. Cloud computing provides the facility for data storing securely[4].

2. Cloud computing provide the solution the need for users for advance gears, it also cause to lower cost of the hardware[4][5].

3. By sharing the piece of equipment amongst of the cloud computing as per their needs[1][3].

4. The cloud services provides the different ways to use the internet services[2][4][6].

SECURITY ISSUES

There are various security issues since cloud computing makes use of so many new technologies, including systems, databases, working frameworks, virtualization, asset planning, and exchange administration. For a larger number of these frameworks and technologies, similar security problems also apply to cloud computing.

The list, according to the RSA conference, which was held in March 2016. The 12 risks of cloud computing are listed below .

Compromised credentials and broken authentication

1. Hacked Interfaces and APIs

2. Exploited system vulnerabilities

3. The APT parasite

4. Inadequate diligence

5. Account Hijacking

6. Permanent data loss

7. Malicious Insiders

8. Cloud services abuses

9. Dos attacks

10. Share technology and Share dangers

Data Breaches:

Because of improved technology, cloud servers can now store more data, making them a target for hackers. As the amount of data exposed rises, so will the harm to society and users. While it is usual for personal information to be disclosed, breaches involving health information, business trade secrets, or intellectual property rights may be more detrimental. Businesses must secure their own data in the cloud, even though cloud service providers frequently offer security measures to protect their environments. Using multi-factor authentication and encoding the data or information to make sure that only authorized users can access it.

Compromised credential sand broken authentication:

Because of advances in technology, cloud servers can now store more data, making them a target for hackers. As the amount of data exposed rises, so will the harm to society and users. Although it is usual for personal information to be disclosed, breaches involving health information, business trade secrets, or intellectual property rights may be more detrimental. Data breaches and other attacks frequently occur as a result of weak passwords, insufficient key or certificate management, or careless authentication methods. Sometimes, not only organizations but even individuals fail to close the access after completing our duties. Take the Gmail account as an example. If we sign in at public access points (internet cafés) and forget to log out after use, our personal information is exposed to others. Our responsibility is to look for ourselves and keep everything in mind. To prevent these issues, multi-factor authentication measures like one-time passwords, phone-based authentications, OTPs, and security questions would make it more challenging for an attacker to log in using stolen credentials. To avoid unauthorized key use and to make it more difficult for attackers to access resources, cryptographic keys should be cycled often. Businesses frequently give the cloud provider control of

protecting their surroundings, but it is ultimately their obligation to safeguard their own data in the cloud.

Hacked Interfaces and APIs:

Currently, APIs are offered by all cloud services. They are utilized to manage, orchestrate, and monitor cloud services. Weak APIs and interfaces would put authorizations at risk with confidentiality, integrity, availability. The CSA advises focusing on threat modelling applications like architecture and design since these are the key ideas for future improvements. They also advise looking at security-coding reviews' weaknesses and high-level testing's shortcomings.

Exploited system vulnerabilities:

We've been worried about bugs for a very long time. You could say that they are constantly being observed in some way. As technology has been utilized more frequently, these vulnerabilities have become more important. Sharing of memory, databases, and other types of information between organizations may cause data loss, the disclosure of more significant faults, and subsequently, maybe, virus exposure. In order to prevent these issues and system vulnerabilities, one will probably need to scan systems, mobile devices, etc. frequently and hunt for patches for the found problems.

Account Hijacking:

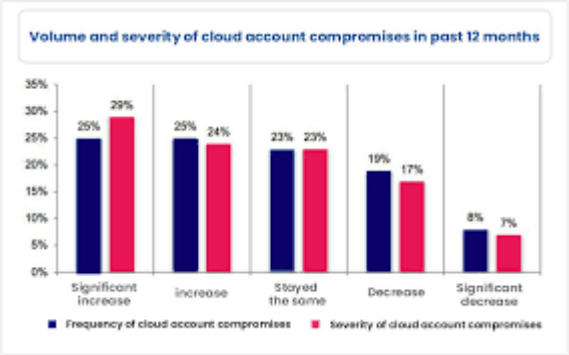


Figure:8: Security concerns with cloud computing.

Account hijacking is one of the most common and frequently discussed issues in today's world. Giving up our login details to others and providing personal information to other parties during online transactions are only two of the many potential grounds for hijacking. Attackers that gain access to our account could possibly change transaction details, manipulate data, and even use other cloud services connected to the account to conduct additional attacks. Currently, all we can do is be cautious when sharing our credentials and follow up frequently when something goes wrong so that we can report it immediately.

Malicious Insiders:

Most frequently, persons who work for or are connected to the organizations and have access to sensitive information that needs to be kept private and secure are the ones that pose these dangers. By limiting requests for access to computer systems during business hours and by encrypting routine actions like scanning, we can at least substantially prevent these insider dangers. Sensitive user data stored on servers mistakenly will surely have a long-term detrimental effect on the company's reputation and business. Therefore, it is crucial that persons in charge of certain regions have adequate training in order to manage those areas without making situations worse.

The APT parasite:

The APT is a continuous hacking operation which is created by individual or group of members and they are attacking on a particular organization. It is mainly use for attacking and hijacking the particular organizations. This procedure employs the viruses and malware throughout the loop holes (viruses, flaws, installs) into the system. It attacked the system by using the different manual programs. The employment of a programmed code which is malware that affected itself to all machines connected to a computer network depending on these security flaws. Recently some issues are coming through in the security issues like USB drive attacks.[2][5]

DOS attacks:

DOS attacks are critically affected the performance of the system directly or anonymously, systems are running out of the time and sometimes it may slower in performance in the working tasks. Because of the DOS attacks the system sometimes behave abnormally, like system run so many programs at a time periods and automatically those programs are open and close respectively, continuously.

RESEARCH CHALLENGES

In every industry, there are still a lot of problems that are difficult to be fixed, and new problems keep

growing up. Here are a few cloud computing research difficulties are following:

1 Cloud data management and security

2 Data Encryption

3 Virtual machines migration

4 Access controls

5 multi-tenancies

Cloud data management and its security:

The concept of cloud data is a specific area of study for cloud computing. Large amounts of unstructured data with infrequent cloud updates are all possible. So, the developer or cloud data manger is the responsible for the secure the cloud data and keep it updated. Auditability is the achieving by testing the particular condition of the sudation. The storage structure and access pattern and application programming are the interface of the file systems, and those are different form the conventional file distribution systems. As a result, there can be compatibility problems are coming.

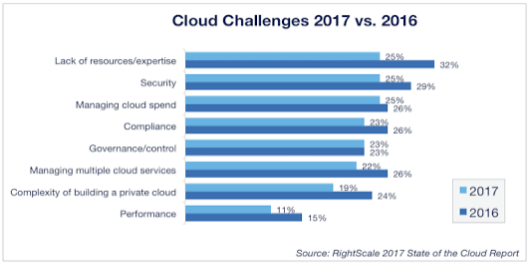


Fig 16: Cloud Challenges.

Data Encryption:

Data encryption is the very specific part of the data security technologies. Security is varied in three phases which are low, medium and high. Those three phases are come in the terms of the expenses of time and issues. If we use the data without the encryption and we are facing the issue of data can be stolen and data is less secure because any malware can be easily entered in the data [4][7]. If we are using the data encryption in cloud data then we can say it is more secure comparatively and no other intermediate malware or viruses can be entered at the time of data transferring.

Virtual machine migrations:

Virtual machine migration is the feature which is handled the load throughout the data transferring by the data centers. Virtual machine migration was introduced in 2011 by Xen and VMW. It causes the resulting data in ten milliseconds. Mostly advantage of the virtual machine migration is the eliminating the hotspot. Virtual machine migrations are handled or manage the unexpected load which is comes throughout the transferring the data by the data centers. Virtual machine migration's main task is the eliminating is the connecting hotspot after the detection of them.

Access Controls:

When we are talking about the managing the security and authentication of data in cloud computing, that are very crucial and define the how strengthen the data is secure. Other thing is that how securely customer claim the password and its strength? What are the recovery techniques use for that? How to secure the username and password and how we secure the messages and other logs without being visible?[5][9] Those term are enhancing the access control of data over the cloud services and provide us more reliability and security with data. This all work done in the term of improvement of the security and will provide the clarity and more functionality in the future.

Multi-tenancy:

Multi-tenancy, due to using same server by the user which is victim and attacker has to be come in physical machine. Because it is not such that entering in to the system and monitoring the inner network layers, such steps are mitigated, which is mitigated by particular security approaches and measurement. It offers so many advantages and disadvantages as well. A resources allocation is made harder to achieve the multi-tenancy for the users [7][4]. Multi-tenancy is easy to achieve by the cloud administrator. By making the multi-tenancy challenges for the cloud users is restricting some attacks and put a limit for the attackers.

Reliability and availability of services:

The concept of reliability is prevalent when a cloud service provider delivers on-demand services. Users mostly depend on network services (network availability in slow signal stages) for dependability and availability. A good example of this is Apple's Mobile Me service, which offers cloud storage and device synchronization features. The result was

initially subpar since numerous users were unable to precisely synchronize the data. In order to get over such problems, providers have moved to technologies like Google Gears and Adobe AIR that allow cloud-based programs to operate with local time. On reliability has made some progress, but it is still challenging to achieve for an IT solution based on cloud computing, especially considering the use and implementation of software like 3D gaming applications and video conferencing systems.

FUTURE ADVANTAGES

In the next five years, the entire IT sector will be moving towards the idea of automation. Artificial Intelligence (AI) and Machine Learning (ML) will most likely play a significant role in the automation process over the course of the next five years. We can anticipate a decline in traditional programming positions in the IT sector as automation continues to advance.

Let's use an example to support the previously described scenario. We can envisage the harm that will be done in terms of INTRUSION when a machine takes control of developing logic during the automation process instead of a human brain. If a traditional programmer wants to use his or her knowledge and skills to take advantage of the computer's resources, it takes a fair length of time to carry out (or) complete the assigned task. But if a computer does the same job using the technology of today and the intelligence it gained via machine learning, it completes the task in a matter of seconds. The conventional IDS systems would no longer be appropriate in this scenario's setting of automation. Therefore, there is a pressing need to reinforce the established security measures such as IDS and fire walls.

In 2022, just 60% of all devices would be using the internet and cloud-based services, according to the report Cyber Security: Threats, Reports and Challenges . By 2025, 90% of devices and industries worldwide are predicted to use the internet and cloud as their primary service providers. This enables us to comprehend that when the number of IOT devices is used, the demand on the cloud also grows. Additionally, this leads to an increase in security problems that can't be resolved by current solutions. We need improvements in security maintenance and fresh studies must be conducted on how to improve cloud security. How can we strengthen our security system? so that everything will be within our control even if a hacker attempts to use new technologies in the automation process to compromise the systems or services.

CONCLUSION

A new technology called cloud computing uses the idea of distributed computing. Although it is not yet fully implemented, this idea will be absolutely essential to the software industry's future. In this essay, we first spoke about what cloud computing is and the various services it offers. Following that, we'll discuss the significance of cloud computing for important industries, security concerns, research obstacles, and cloud computing applications and future developments. We have noted that there are a number of security issues, including network and virtualization security concerns. This essay has outlined all the security concerns with cloud computing as well as possible solutions. To be compatible with cloud architecture, new security technologies must be created and existing ones must undergo significant modification. We think that businesses use cloud services most frequently in the industrial sector. This paper examines the growth in cloud usage from 2015 to 2017 as well as cloud utilization in five major industries. Last but not least, as the entire IT industry anticipates the process of automation, we have offered an overview of what we envision it would be like and what the fundamental security challenges that will be encountered in the future. We anticipate that our work will contribute to a better understanding of design difficulties in cloud computing and open the door for additional research in this field because automation in cloud computing is still an ideal process that requires more clarification and investigation.

REFERENCE

[1] "Emerging Advancement and Challenges in Science, Technology and Management " 23rd & 24th April, 2021

[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 Narayana Reddy G," Cloud computing-types of cloud," 2013, Retrieved from http://bigdatariding.blogspot.my/2013/10/cloudcomputingtypes-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