# Cloud Computing: Security and Privacy Challenges

**Sandeep Sutradhar**

*Dept of Computer Science, MCA.*

*Christ (Deemed to be University)*

Bangalore, India

sandeep.sutradhar@mca.christuniversity.in

***Abstract*—Cloud Computing has been the buzzword in the recent decade. It is growing like never before. Distributed systems have their own advantages and disadvantages. In terms of its usage for different purposes, it is dominating society. But like every technology which is dependent on the internet, it is also having some security issues which can have a drastic effect on the data available to the cloud platform. So, we are facing some challenges regarding cloud service. Though we are trying to find the proper solution for each of its problems, this field is still in development, and the work is going on continuously.**

***Keywords—Cloud Challenges, Cloud computing, Security and Privacy, threats, cloud management, migration***

## I. Introduction

The term cloud means a Network or the Internet. In other words, we may say that cloud is something, which is present at a remote location, or we may say that cloud computing means to use of someone else's Computer. Cloud can provide many services over public and private networks, like WAN, LAN, VPN, etc. Applications such as e-mail, web conferencing, and customer relationship management (CRM) execute on the cloud. Cloud Computing means configuring, manipulating, and accessing the hardware and software resources remotely. It offers services like online data storage, infrastructure, application, etc. Cloud computing offers platform independency as well, as the software need not be required to be installed locally on the personal system. Hence, we may say that Cloud Computing is making our business applications mobile and collaborative.

There are a few benefits of cloud servicing, which have been shown in the figure [1].

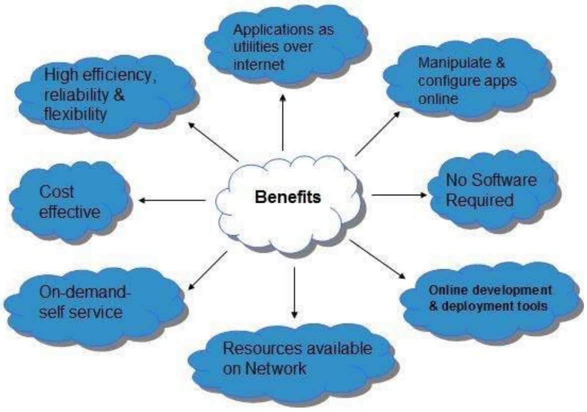

Applications as utilities over internet
High efficiency, reliability & flexibility
Manipulate & configure apps online
Cost effective
Benefits
No Software Required
On-demand-self service
Online development & deployment tools
Resources available on Network

*Fig 1. Benefits of Cloud Service*

Cloud computing is a highly fast-growing technology with a sea of possibilities and business opportunities around the globe [2]. But as we know, like every rose has its thorn, In cloud setting up, the cloud business has its challenges. Here in this paper, the main focus is to discuss the challenges available for cloud computing in our daily life.

## II. Challenges in Cloud Computing

Despite all the developments and potential power of cloud computing services, there are multiple existing challenges of cloud computing services that many businesses face. Here we are compiling a list of challenges of cloud services [3] that need to be taken care of leverage the maximum capacity of the cloud.

1. Security and Privacy
2. Password Security
3. Cost Management
4. Lack of expertise
5. Internet Connectivity
6. Control or Governance
7. Compliance
8. Multiple Cloud Management
9. Creating a private cloud
10. Performance
11. Migration
12. Interoperability and Portability
13. Reliability and High Availability
14. Hybrid-Cloud Complexity

### *A. Security and Privacy*

The topmost concern in the cloud is security issues in cloud computing services. It is because our data gets stored and processed by different vendors, and we cannot see it. Every day or the other, we get informed about broken, compromised credentials, account hacking, authentication, data breaches, etc., in a particular organization. It makes us a little more skeptical. Like all other branches of technology, security and privacy are pressing concerns in the world of cloud-based computing as well since we cannot see where our data is being processed or stored [4]. This even increases the risks which can arise during the management or implementation process. Currently, 93% (According to a study)of leading companies across various sectors are highly concerned about facing a significant data breach within their cloud-centric ecosystems [5]. However, These challenges can be reduced using security applications, encrypted file systems, and data loss software. Fortunately, cloud providers nowadays have started to improve security capabilities at a higher rate. You can also stay cautious by verifying if the cloud provider implements safe access control and safe procedures user identity management system [6]. Also, you may ensure whether it implements database security and privacy protocols.

### B. Password Security

Since dealing with cloud computing means sending and receiving large amounts of data at high speed and accuracy, the communication channel can also be responsible for data leaks. Data security and integrity issues can include identity theft, malware infections, breaches, hacking and other threats [7]. These breaches can eventually lead to a potential loss of trust from the clients in any service. Here the organization should use a multiple-level authentication and can ensure that the passwords remain protected by applying various techniques. Also, the passwords should be modified in an interval of time, especially when a particular employee leaves or resign from the organization. Access rights of usernames and passwords should be given judiciously to the employees [8]. As many people access the cloud account, it may become vulnerable. Anybody with your password or hacks into the cloud account can access your confidential information.

### C. Cost Management

Cloud computing enables us to access the application software over a fast internet connection and also lets us save on investing in costly computer software, hardware, management, and maintenance [9]. This makes the service affordable. But what is expensive and challenging is tuning the organization's needs and working on the third-party platform. Another costly matter is the cost of transferring data and services to a public cloud, especially for any small business or project; as we know already that cloud service providers charge the cost according to the time the service has been used. So if some organization is using the service for a more extended time, then the price might not be affordable for the organization [10]. So, a business should be able to make the decision according to their use [11].

### D. Lack of expertise

Management is becoming difficult with the increasing workload on cloud services and continuously improving cloud tools for a better customer experience. There has been a high demand for a trained and skilled workforce who can deal with cloud computing services and tools. Hence, firms need to train their experienced staff in order to minimize this challenge. SME (small and medium-sized) organizations may add specialists to their IT teams to be cost-effective [12]. But, many everyday tasks these specialists perform can be automated by different tools. To this end, many companies are turning to DevOps tools, such as Chef and Puppet, to perform various tasks, such as automated backups at predefined periods and monitoring continuous usage patterns of resources. These tools can also help optimize the cloud for governance, cost, and security.

### E. Internet Connectivity

Cloud services are highly dependent on a high-speed internet connection. So businesses that are relatively small and face connectivity issues should first invest a good amount of budget in a good and stable internet connection so that no downtime happens in their business because internet downtime might create vast business losses since Performance is an essential factor in cloud-based solutions or cloud business. If the Performance of the cloud service is not good enough for all the customers, it can fade away from the users and decrease the profits. Any organization or individual will not be keen on compromising the quality and sustainability of the services [13]. Even though it is hard to mitigate all kinds of server outages, constant monitoring can prove to be helpful in reducing the downtime rate. You can tackle the problem with proper cloud monitoring tools that can be used to monitor your Cloud's Performance constantly. However, even though there are multiple cloud monitoring tools in the market, many of them can be more expensive.

### F. Control or Governance

One of the ethical issues in cloud computing is maintaining proper asset management and maintenance control [3]. In today's cloud-based era, technology does not always have complete control over the provisioning, de-provisioning, and all the infrastructure operations. And this has increased the difficulty for IT to provide the compliance, governance, risks, and data quality management required for any business. To mitigate the challenge, there should be a dedicated team who can ensure that the assets used for implementing cloud services are being used according to the agreed policies and reliable procedures [4]. There should be proper maintenance, and the assets should be used to achieve the organization's goals successfully and efficiently.

### G. Compliance

One of the significant risks of cloud computing is maintaining compliance. The term Compliance means a set of rules about what and how much data should be allowed to be moved and, at the same time, what should be kept in-house. The organizations must follow and respect all the compliance rules which various government bodies and organizations have set. This is an issue for anyone using backup services or storage. Every time a company transfers data from internal storage to a cloud or vice versa for backup, it is faced with compliance with all official regulations and laws [14]. Like, healthcare organizations in the USA have to comply with HIPAA (i.e., Health Insurance Portability and Accountability, which was the Act of 1996), public retail companies will have to comply with SOX (i.e., Sarbanes-Oxley, an Act of 2002), and PCI DSS (i.e., Payment Card Industry Data Security Standard). It depends on the sector and requirements that every organization must ensure all these standards are respected and carried out. So, the Customers need to look for vendors who can provide compliance and also check if they are also regulated by the standards they need. Some of the vendors offer certified compliance, but in some cases, some additional input is required on both sides to ensure all the proper compliance regulations.

### H. Multiple Cloud Management

The Challenges facing cloud computing haven't just been concentrated in just one single cloud service. The need for multi-cloud has grown exponentially in recent decades. Companies have already started to invest in multiple private clouds, public clouds, or a combination of both is called the Hybrid Cloud. And tech giants like Alibaba and Amazon are leading the way [15]. On average, companies use about 4-5 private and public clouds, which can prove difficult to manage for the infrastructure team. This has grown rapidly in recent times. So it has become important to list the challenges faced by such organizations or groups and find solutions to grow with the trend.

### *I. Creating a private cloud*

Implementing an internal cloud is advantageous for many sectors. This is because all the data can remains secure in-house with the organization. But the major challenge in this is the IT team has to build from zero to everything and also fix everything by themselves [16]. Also, the team needs to ensure the smooth functioning of the cloud without any data loss. They need to automate maximum manual tasks to save time. The execution of tasks also should be in the correct order as well. So at this moment, it sounds quite challenging to set up a fully private cloud all by ourselves. But many organizations will definitely do so in the future.

### *J. Performance*

As When your business applications move to a cloud or a third-party vendor, so your business performance, along with the security, starts to depend on the cloud provider as well. So, Another major problem in cloud service is investing in the right cloud service provider. Before investing, you should look for providers with innovative technologies. The Performance of the BI's (Business Intelligence) and other cloud-based systems are fully linked to the provider's systems as well(maybe remotely). Be cautious about choosing the correct provider and investigate whether they have the protocols to mitigate issues that arise in real-time. Since Performance is an important factor when considering cloud-based solutions [16]. If the Performance of the cloud services is not satisfactory, it can move away users and decrease the profits of the business. Even a small latency while loading an app or a web page may result in a huge drop in the percentage of users in sales for e-commerce. This latency can be a product of inefficient load balancing, which means that the server cannot efficiently split the incoming traffic so as to provide the best user experience. Challenges also arise in the case of fault tolerance, which means the operations continue as required even when one or more of the components fail.

### *K. Migration*

Migration is one of the leading Cloud computing sector issues in recent times. Actually, this is the process of moving or copying an application to the Cloud system. Although moving a newly made application is a straightforward process, but when it comes to moving an existing application(s) to a new environment(i.e., cloud), many cloud difficulties arise and which in turn make it difficult [18]. Many leading companies are currently migrating their application(s) to cloud-based services. Interestingly over half of them find this more difficult than expected – since projects are over budget and deadline needs to match. Velostrata conducted a survey recently wherein they found that 95% of organizations are moving their application(s) to the cloud. The survey showed that most organizations or companies are finding it a nightmare to migrate. Some notable issues faced here are security challenges in cloud computing, extensive troubleshooting, slow data migrations, application downtime, migration agents, and cutover complexity.

### *L. Interoperability and Portability*

Since one of the major challenges of cloud computing is that application(s) need to be easily migrated between cloud providers and also without being locked for a set period. And there is a lack of flexibility and availability in moving from one cloud provider to the other because of the reason of complexity involved in the process. There must not be vendor lock-in. Although, it is not yet made possible because each cloud provider uses different standard languages for their platforms. Since, Changing cloud inventions bring a slew of new challenges, like establishing a secure network from scratch, managing data movement, etc. And the other challenge is customers can't access it from everywhere. The application(s) on one platform(cloud service provider) should be able to incorporate services from the other platforms. It is possible via web services [19], but developing such web services is very complex. However, this can be fixed by the cloud providers [20] so that the customer can securely get access to the cloud from anywhere.

### *M. Reliability and High Availability*

Most businesses are dependent on services provided by third-party. Hence the cloud systems must be reliable and robust. Some of the most pressing challenges in cloud computing are the need for reliability and high availability (HA). Reliability may refer to the likelihood that the system will be up and start running at any given point in time. In contrast, availability may refer to how likely it is that the system or nodes will be up and start running at any given point in time. As we migrate towards an age where about 94% of businesses are using cloud-based service providers (CSPs) or platforms in some way, and it is growing up exponentially, shape or form, being able to ensure that the right and accurate data is available at any given point of time while on the other hand retaining system functionality and work has emerged as one of the significant problems with cloud computing. Because most businesses nowadays are reliant on third-party services [21], cloud services must be dependable and robust all the time. Cloud providers continue to lack round-the-clock service, which results in frequent outages. It is also difficult to use internal or third-party tools for monitoring the service being provided all the time. It is critical to have plans also in place to monitor SLAs, robustness, Performance, usage, and business reliance on these services as well.

### *N. Hybrid-Cloud Complexity*

Last but not least, For any organization, a hybrid cloud environment is a messy mix of multiple cloud service providers and cloud application development, as well as public and private clouds, all are operating at once. The combination of a common user interface, consistent data, and, most importantly, analytical benefits for businesses are missing from these complex cloud service ecosystems. Some Cloud computing challenges like integration, scalability, and disaster recovery are all magnified in a hybrid cloud environment. When it comes down to investing in or starting a cloud business vertical, many people might face business development as an important challenge to tackle. It might be because of not have the proper experience or maybe because you are not completely aware of the scaling possibilities.

There exist many ways you can go about scaling your business. You can reach out to them directly or connect with them digitally; lead generation and developing a sales channel can be a way to go about it. Try to also position yourself smartly in the market by highlighting your USP. Focus on segmenting your customers and targeting them accordingly. You can also educate yourself and your team more about marketing, sales, and the business development process.

## III. DATA SECURITY AND PRIVACY CHALLENGES

We know that Cloud computing environments are kind of multidomain environments in which each domain uses different security, privacy, and trust requirements and potentially employs various interfaces, mechanisms, and semantics. All the domains could represent the individually enabled services or other infrastructural or application components. Information security is concerned with protecting the integrity, confidentiality, and availability of data regardless of the form the data may take [22]. Security is more complex in a virtualized environment because we now have to keep track of security on two tiers, i.e., the physical host security and the virtual machine security. And it is a fact that if the physical host server's security is compromised, then all of the virtual machines residing on that particular host server are impacted. And a compromised virtual machine might also wreak havoc on the physical host server, which may then have an ill effect on all of the other virtual machines running on that same host [23]. While the cloud offers several advantages, people come to the cloud computing topic from different points of view. Some believe that a cloud is an unsafe place. But few people find it safer than their own security provisioning, especially small businesses that do not have the resources to ensure the necessary security themselves. Since the cloud is being used by organizations and individuals as well at an extensive rate, some users even store common, private, and sensitive data in the cloud. Data theft is one of the major issues faced by cloud providers because, as we discussed above, nowadays, data in the cloud can be accessed anytime, anywhere. The cloud computing service provider must enforce their own policies to ensure the safety of the data users stored in their cloud model. They must make sure that they realize who is actually accessing the data stored in the cloud and only the authorized person can maintain the cloud service model [24]. There are several kinds of security threats as well as privacy concerns, but this paper has tried to cover the most common and critical ones.

### *A. Insider Threats*

It is a well-known fact that most security threats arise from within an organization, as shown in figure 1 [25]. This threat is many folded for consumers of cloud services since; the cloud is based on the multi-tenant model under the provider's single management domain. To top it all, the organizations which subscribe to cloud services usually lack transparency into the provider's processes to hire its employees, keeping data in different locations, and its relationships with third-party vendors. There is often no visibility into the hiring standards and practices for cloud employees [26] by the cloud provider to its consumers.

### *B. Outside Malicious Attacks*

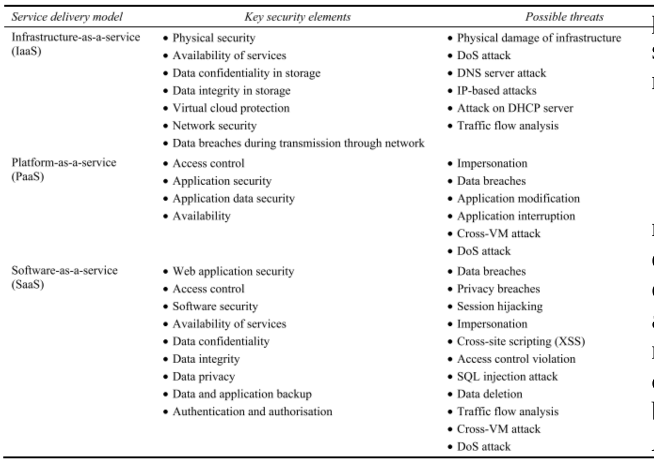
It is Outside threats are one of the most concerning issues with any organization since it directly entails the release of confidential information out in the open or possible defacing of the organization. This is one of the persistent issues in Cloud infrastructure as well since Clouds are more associable than private networks and have more interfaces to help its legitimate users access information. This very fact is what the hackers and attackers leverage to their advantage by exploiting the API [27] weakness, connection (media or logical channel) tapping or breaking in, and by social engineering. The outside attacks may not be as damaging as inside attacks; however, they are the most difficult to conceal.

### *C. Service Disruption*

While service hijacking is not new, even with Cloud infrastructure, malicious attacks such as phishing, fraud, and exploitation of software vulnerabilities still help hackers score. Even worse, an attacker can replay sessions and redirect an organization's clients to illegitimate sites or launch a Denial of Service (DoS) or Distributed DoS (DDoS) attack leveraging bot-nets and auto-dialers. The soft targets are the machines that are connected to the outside world and the IP addresses and extensions that are exposed via various publically available internet tools (e.g., WHOIS). The worse part still, these compromised accounts can become a launching base for the attacker [28] from where he can leverage a legit account to launch subsequent attacks, which will go unnoticed, and the attacker will be concealed.

### *D. Physical-level security issues*

Securing the physical infrastructure of the cloud is an important aspect, as it may lead to various security and performance issues. Sometimes the competitor organizations may try to disrupt the services of a cloud provider by intentionally damaging its physical infrastructure (e.g., networking components). Cloud infrastructure may also get damaged due to natural calamities like floods, storms, etc. Therefore, to avoid such losses, a cloud service provider must survey different geographical locations where he/she wants to set up his/her organization. The reliability of hardware is always the prime concern for cloud service providers. Unreliable hardware may affect the smooth and trouble-free operation of cloud services. The following figure (Fig 2.) shows the security issues in cloud service delivery models [29]



| *Service delivery model* | *Key security elements* | *Possible threats* |
|---|---|---|
| Infrastructure-as-a-service (IaaS) | • Physical security<br>• Availability of services<br>• Data confidentiality in storage<br>• Data integrity in storage<br>• Virtual cloud protection<br>• Network security<br>• Data breaches during transmission through network | • Physical damage of infrastructure<br>• DoS attack<br>• DNS server attack<br>• IP-based attacks<br>• Attack on DHCP server<br>• Traffic flow analysis |
| Platform-as-a-service (PaaS) | • Access control<br>• Application security<br>• Application data security<br>• Availability | • Impersonation<br>• Data breaches<br>• Application modification<br>• Application interruption<br>• Cross-VM attack<br>• DoS attack |
| Software-as-a-service (SaaS) | • Web application security<br>• Access control<br>• Software security<br>• Availability of services<br>• Data confidentiality<br>• Data integrity<br>• Data privacy<br>• Data and application backup<br>• Authentication and authorisation | • Data breaches<br>• Privacy breaches<br>• Session hijacking<br>• Impersonation<br>• Cross-site scripting (XSS)<br>• Access control violation<br>• SQL injection attack<br>• Data deletion<br>• Traffic flow analysis<br>• Cross-VM attack<br>• DoS attack |

*Fig 2. security issues in cloud service delivery models*

### E. Physical Data storage-related security issues

Data in storage can be compromised by exploiting weaknesses in the algorithms used for logical partitioning. Since In a cloud computing environment, users' data are stored at different geographical locations. This prevents cloud customers from deploying their own data security solutions. Therefore, complete data security depends on the measures taken by the cloud service providers. Users' sensitive data in storage and computation-related data must be properly segregated. Weak user data segregation may lead to various security issues like data leakage, data theft, etc. After a VM is shut down, all the data associated with that VM must be properly disposed of. Many times even after shutting down a VM, its data is still present in the memory, which may lead to serious data security problems.

### F. Digital security authentication mechanisms

Similarly, digital authentication is used when an individual or online entity is honest with the service provider or when it seems that the mechanism is suitably established [30]. One of the mathematical schemes that provide verification and authentication of any kind of digital message is a digital signature. The digital signature is a kind of cryptographic value calculated from the data and a secret key that is known only by the signer. Credentials work as pieces of evidence of authority, entitlements, status, and access rights. They provide particular users with a piece of evidence to prove that they are right to use resources and services. In fact, taking advantage of credentials (such as one-time passwords, patterns, and captchas) is a traditional way of securing malicious activities.

### G. Human Factor

At first, glance, reinforcing the security of the cloud provides a secure infrastructure for information. In cloud systems, the human access level to the system is different, so an employee or customer with an administrator access level can play a critical role in saving or damaging system security. To fix security threats and eliminate vulnerabilities, in addition to technological defects, human mistakes and behaviors should definitely be considered. With more emphasis on human behavior, a vulnerability pattern (such as social engineering) can be found [31]. Then, social engineering attacks will be monitored and studied in more detail.

### H. Segregation

One of the major characteristics of cloud computing is multi-tenancy. Since multi-tenancy allows the storage of data by multiple users on cloud servers, there is a possibility of data intrusion. By injecting a client code or by using any application, data can be intruded upon. So there is a necessity to store data separately from the remaining customer's data. Vulnerabilities with data segregation can be detected or found using the tests such as SQL injection AWS, Data validation, and insecure storage.

### I. Data-Centric Security and Privacy

Since data in the cloud typically resides in a shared environment, but data owners should have full control over who has the right to use the given data and also what they are actually allowed to do with the data once they gain access to it . To provide data control in the cloud, a standard-based heterogeneous data-centric security technique is an essential element that shifts data protection from all the systems and applications. Hence, documents must be self-describing and defending regardless of their environments. of data intrusion. [32] It is a fact that multiple service providers coexist in clouds, and sometimes they collaborate to provide various services; there is a high chance that they might have different security approaches and privacy mechanisms for all users, so we must address heterogeneity among their policies.

### J. Instance Isolation

Isolation ensures that different instances which are running on the same physical machine must be isolated from each other. Virtualization efficiencies in the cloud require virtual machines from multiple organizations to be co-located on the same physical resources. Although traditional data center security still applies in the cloud environment, physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server. Administrative access is through the internet rather than the controlled and restricted direct or on-premises connection that is adhered to in the traditional data center model. This increased risk of exposure will require stringent monitoring for changes in system control and access control restriction [33]. The isolation is done via the Xen hypervisor.

## IV. CURRENT SECURITY MEASURES

In order to deal with the above-mentioned problems or issues, there are certain measures that are followed by organizations in order to protect their data from theft or any kind of damage [34].

### A. Privacy data access processing

Although the combination of the public and private clouds are a reasonable scheme to deal with cloud computing security and privacy, but how to effectively integrate the two types of clouds is still a tough problem. The ideal object is composed of two parts. On one side, we are able to make adequate use of the rich computing and storage resources of the public cloud. On the other hand, the privacy information of the clients should be protected effectively. The community cloud is composed of two or more clouds running independently, which supports the data and application transfer among different clouds. The community cloud, which consists of private cloud and public cloud, has both advantages; namely, it has not only the private property of the private cloud but also the low computational costs of the public cloud. As a result, the community cloud has become the preferred pattern for many corporations or organizations, and it is regarded as the prime mode of future cloud computing as well.

### *B. Encoding data searching*

Early references involved a encrypt data searching-based The practical algorithm adopts a symmetric encryption algorithm to encode the text and its keywords, respectively. The server can search which texts include the corresponding keywords offered by the clients, but it cannot obtain practical information on the text content. Moreover, the current search scheme can only complete searching of a single keyword, but it cannot satisfy the common search of the clients. In order to guarantee that the public-key encryption with keyword searching can be better applicable to the cloud computing environments, we should construct another better public-key encryption scheme that can realize privacy protection and complex logic expression.

### *C. Encoding data computing*

With the fast development of cloud computing, the data owner is able to upload massive data to the cloud server to conduct computing and searching, which is helpful in decreasing the costs of storage, computation, and management. Recently, property encryption and homomorphic encryption have been utilized to deal with the issue of encoding data computing. Homomorphic encryption is to conduct the cipher text and the plaintext simultaneously and directly. With this algorithm, the cipher text can still be done even though the plaintext is unknown. The clients encode the data first, and then the cipher text is uploaded to the cloud server. The server can conduct the data cipher text according to the client's requirements and put the computed result to the clients. The clients can use the private key to decode the cipher text to achieve the corresponding computed result of the plaintext. However, the clients cannot verify the correctness of the computed result from the cloud server.

## V. CONCLUSION AND FUTURE WORK

It is undeniable that cloud computing has brought us lots of benefits and becoming more popular nowadays. Many large companies have started using cloud services in their business. While cloud computing is widely used, security becomes a concern to everyone who uses cloud services. There is a lot of security that arises continuously while there are improvements as well on the security model of all the cloud services and components. In the increasing use of the cloud service, the user should also use the cloud service provided wisely in a way that always ensures good security practices so that the following technology has the potential to bring information technology to the next level. Also, it should keep in mind that data privacy and its security is not only the responsibility of the service providers but of the user as well.

## REFERENCES

[1] https://www.tutorialspoint.com/cloud_computing/cloud_computing_overview.html

[2] Mohsen Attaran, Sharmin Attaran, and Bilge Gokhan Celik, "Promises and Challenges of Cloud Computing in Higher Education: A Practical Guide for Implementation."Journal of Higher Education Theory and Practice Vol. 17(6) 2017.

[3] Tharam Dillon and Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges," 1550-445X/10 $26.00 © 2010 IEEE DOI 10.1109/AINA.2010.187, 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[4] David C. Wyld1, "The cloudy future of government IT: cloud computing and the public sector around the world," International Journal of Web & Semantic Technology, vol 1, issue 1, January 2010.

[5] https://www.datapine.com/blog/cloud-computing-risks-and-challenges/

[6] J. C. Roberts and W. Al-Hamdani, "Who Can You Trust in the Cloud? A Review of Security Issues within Cloud Computing," Proceedings of the 2011 Information Security Curriculum Development Conference, Kennesaw, 7-9 October 2011, pp. 15-19. doi:10.1145/2047456.2047458

[7] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, Vol. 16, No. 1, 2012, pp. 69-73. doi:10.1109/MIC.2012.14

[8] A. Kim, J. McDermott and M. Kang, "Security and Ar- architectural Issues for National Security Cloud Computing," Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops, Genova, 21-25 June 2010, pp. 21-25.

[9] M. Mathur, "Elucidation of Upcoming Traffic Problems in Cloud Computing," Recent Trends in Networks and Communications, Communications in Computer and Information Science, Vol. 90, 2010, pp. 68-79.

[10] K. Rafique, A. W. Tareen, M. Saeed, J. Z. Wu, and S. S. Qureshi, "Cloud Computing Economics Opportunities and Challenges," 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC- BNMT), Shenzhen, 28-30 October 2011, pp. 401-406. doi:10.1109/ICBNMT.2011.6155965

[11] Rafael Moreno-Vozmediano, Rubén S. Montero, and Ignacio M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services",Digital Object Indentifier 10.1109/MIC.2012.69 1089-7801/$26.00 2011 IEEE

[12] Ali Khajeh-Hosseini, Ian Sommerville, and Ilango Sriram, "Research Challenges for Enterprise Cloud Computing."

[13] R. Moreno-Vozmediano, R. Montero and I. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services," IEEE Internet Computing, 18 May 2012. http://doi.ieeecomputersociety.org/10.1109/MIC.2012.69

[14] Aprna Tripathi and Bhawana Parihar, "E-Governance challenges and cloud benefit," 978-1-4244-8728-8/11/$26.00 ©2011 IEEE.

[15] J. F. Yang and Z. B. Chen, "Cloud Computing Research and Security Issues," International Conference on Computational Intelligence and Software Engineering (CiSE), Wuhan, 10-12 December 2010, pp. 1-3

[16] Faraz Fatemi Moghaddam, Mohammad Ahmad, Samira Sarvari, Mohammad Eslami, Ali Golkar," Cloud Computing Challenges and Opportunities: A Survey," 978-1-4799-7315-6/15/$31.00 ©2015 IEEE,2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN)

[17] Divyakant Agrawal, Amr El Abbadi, Shyam Antony, and Sudipto Das,"Data Management Challenges in Cloud Computing Infrastructures",S. Kikuchi, S. Sachdeva, and S. Bhalla (Eds.): DNIS 2010, LNCS 5999, pp. 1–10, 2010. ?c Springer-Verlag Berlin Heidelberg 2010

[18] A. Khajeh-Hosseini, D. Greenwood, and I. Sommerville, "Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS," in proc. Of IEEE 3rd International Conference on Cloud Computing (CLOUD), Miami, FL, 2010, pp.450-457.

[19] Yi Wei and M. Brian Blake, "Service-Oriented Computing and Cloud ComputingChallenges and Opportunities," Published by the IEEE Computer Society 1089-7801/10/$26.00 © 2010 IEEE IEEE INTERNET COMPUTING

[20] A. Cardoso and P. Simões, "Cloud Computing: Concepts, Technologies, and Challenges, Virtual and Networked Organizations, Emergent Technologies and Tools," Vol. 248, Springer, Berlin, 2012, pp. 127-136. doi:10.1007/978-3-642-31800-9_14

[21] C. Fehling, F. Leymann, R. Retter, W. Schupeck, and P. Arbitter, “Chapter 2: Cloud Computing Fundamentals,” Cloud Computing Patterns: Fundamentals to Design, Build, and Manage Cloud Applications, Springer Press, pp. 21-75, 2014.

[22] Amazon White Paper, http://aws.amazon.com/about-aws/whats-new/2009/06/08/new-aws-security-center-and-security- whitepaper/ , published June 2009

[23] L. Ertaul1, S. Singhal2, and G. Saldamli, "Security Challenges in Cloud Computing."

[24] Hamlen K, Kantarcioglu M, Khan L, and Thuraisingham B 2012 "Security issues for cloud computing Optimizing Information Security and Advancing Privacy Assurance: New Technologies" 8 150-162

[25] Cloud and Telecom security article http://sbin.cn/blog/2009/11/10/true-or-false-70-of-security-incidents-are-due-to-insider-threats/

[26] ISACA (auditor’s perspective journal) http://www.isaca.org/Journal/Past-Issues/2009/Volume-6/Pages/Cloud-Computing-An-Auditor-s-Perspective1.aspx

[27] Research paper – “Private Virtual Infrastructure (PVI) Model for Cloud Computing" International Journal of Software Engineering Research & Practices Vol.1, Issue 1, Jan 2011

[28] Akhil Behl, "Emerging Security Challenges in Cloud Computing An insight to Cloud security challenges and their mitigation," 2011 World Congress on Information and Communication Technologies, 978-1-4673-0126-8/11/$26.00 c? 2011 IEEE

[29] Kriti Bhushan and B.B. Gupta, " Security challenges in cloud computing: state-of-art," Int. J. Big Data Intelligence, Vol. 4, No. 2, 2017, Copyright © 2017 Inderscience Enterprises Ltd.

[30] Khalil I, Khreishah A, Azeem M (2014) Consolidated identity management system for secure mobile cloud computing. Comput Netw 65:99–110

[31] Hamed Tabrizchi1 and· Marjan Kuchaki Rafsanjani1, "A survey on security challenges in cloud computing: issues, threats, and solutions," The Journal of Supercomputing https://doi.org/10.1007/s11227-020-03213-1,Springer Science+Business Media, LLC, part of Springer Nature 2020

[32] Hassan Takabi, James b.d. Joshi and Gail-Joon, "Security and Privacy Challenges in Cloud Computing Environments Cloud," COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES, 1540-7993/10/$26.00 © 2010 IEEE, NOVEMBER/DECEMBER 2010

[33] John W. Rittinghouse, James F. Ransome, “Cloud Computing Implementation, Management, and Security," CRC Press, August 17, 2009, ISBN 9781439806807, pp. 147-158, 183-212.