A REVIEW OVER SECURITY AWARENESS AND CHALLENGES OF CLOUD COMPUTING TECHNOLOGY

Tahir Muzaffar
8 Technologist Karachi, Pakistan
E-mail: tahirmama8@gmail.com

Ushna Ali
National Incubation NEP NIC Karachi, Pakistan
E-mail: ushna668@gmail.com

Muhammad Waqas
Sukkur IBA University Sukkur, Pakistan
E-mail: muhammad.waqaspn@gmail.com

Muhammad Shahbaz
National Incubation NEP NIC Karachi, Pakistan
E-mail: azizterai32@gmail.com

Moiz Khan
8 Technologist Karachi, Pakistan
E-mail: moizsmiu@gmail.com

Usama Khan
8 Technologist Karachi, Pakistan
E-mail: usamak2124@gmail.com

Received: 28h August, 2022; Accepted: 20th January, 2023; Published: 28th February, 2023

***Abstract*:** With the technological advancement in the current era, smart devices have been involved in every sector of human life such as industries, hospitals, institutions, and homes. This massive usage of smart devices has caused an increment in data generation. High-performance computing (HPC) is required to deal with this huge amount of data. Now, it is very costly for small industries and laymen to purchase such types of high-performance computing systems. For this reason, cloud computing is the best cost-effective solution to solve this high-performance computing requirement. In this paper, the authors concentrated on different aspects of cloud computing, a distributed architecture to perform as the centralized server resource on a scalable platform to deliver on-demand computing resources and services. This research paper presented a short overview of cloud computing deployment models, cloud types, cloud services, and the primary security threats and challenges plaguing the cloud computing sector.

Index Terms: Cloud Computing, Smart Devices, Distributed Architecture, Cloud Computing Deployment Models and Services.

1. INTRODUCTION

The Interconnected network of distributed servers is term as cloud computing and provide services as a central point. The primary goal of cloud computing is to remotely access software, resources, and data. The Internet acts as an invisible link connecting all these types of equipment. This probably applies to all virtual and physical servers globally. Cloud computing has emerged as one of the most interesting fields in today's world IT industry. The arrival of cloud computing technology has restructured computing power since it offers enhanced dependability, massive scalability, and lower prices, which has gained the attention of firms and users.

Cloud computing is playing a very key role in the information technology industry. The term "cloud" refers to an Internet-accessible structure that is concealed from users. With the use of cloud computing, users can easily transfer their valuable data and programs to a remote server from which they may retrieve their data anytime and anywhere in a non-complex and remote manner [1]. This is one of the other use cases for central processing. Approximately 50 years ago, a time-sharing computation server supported a wide range of users in a similar condition. Applications and data were stored in local resources in huge before personal computers arrival occurred. The Cloud computing model is not a history repeating currently. Due to the unavailable of enough resources for computing 50 years ago, we had no choice but to use time-sharing servers. Because of the need to develop sophisticated Information technology (IT) infrastructures, cloud computing has been uncommon in past years. A variety of program installations, upgrades, and configurations are to be managed by users.

In simple terms, a collection of various ubiquitous servers is cloud computing that delivers hosting and storage services through the internet [2]. Computing resources and certain other technology are rapidly becoming unpopular and useless. Resulting, computing platform outsourcing is a better choice for users who must manage complex IT infrastructures. The three categories of clouds are public, private, and hybrid clouds. With the growing popularity of cloud-based systems, cloud providers have focused on ensuring consistency, security, privacy, and cost-effective cloud architecture. The resources that are requested as services define the requirements for cloud applications. As a result, the resources might include intensive processing, big storage, and high-volume network resources, among other things [3].

The power of cloud computing has enhanced Information Technology's capabilities. Cloud computing has evolved significantly in the Information Technology industry during the last several years [4]. Along with its many advantages, cloud computing creates a far more difficult situation in terms of the security of data, data confidentiality, authorized access, and so on. The security challenges associated with cloud computing are making it more difficult for users today [5, 6]. The flexibility and advantages of cloud computing will have little credibility if security is not reliable and consistent.

The National Institute of Science and Technology (NIST), defined the definition of cloud computing as "the model which enables the computing convenient, ubiquitous, a shared pool of easily accessible network of configurable computing resources which are available on demand basis (e.g., servers, services, storage, networks, and applications) and can be rapidly provisioned. This can be released with very simple interactions of a service provider or minimal management efforts". [5, 7]

As the usage of cloud computing increased, it also attracted many attackers and hackers' attention to breach the security holes in this paradigm. Botnets are a network of bots, which replicates themselves to spread malware and spam in computing devices, which is an example of a security threat [8]. Nearly 63 percent of the 761 data breaches probed by the US Secret Service in 2010 happened at businesses with 100 or fewer workers [9]. A 2011 survey of midsize and small 2,000+ businesses by security systems supplier Symantec Corp. investigated that over 73% of businesses had been compromised by a cyber-attack [10]. The pay-as-you-go model of cloud computing is one of the most fantastic models which offers computing as a resource. This research paper presents an overview of cloud computing ideas as well as the security challenges that arise while using cloud computing and cloud infrastructure & its solutions.

This paper has been arranged in which section 2, describes the background and characteristics of cloud computing. Section 3 and 4 elaborate on the service and deployment models of cloud computing. Section 5 and 6 highlight the security factors and challenges of cloud computing. Section 7 and 8 mentions the solutions and benefits of cloud computing. In the last, a conclusion has been provided in section 9.

2. BACKGROUND AND CHARACTERISTICS OF CLOUD COMPUTING

In 1960, John McCarthy addressed at MIT, suggested that computing, like electricity and water, and should be treated as a kind of utility item. The company Salesforce started releasing applications to its consumers through a user-friendly web in the year 1999. In the year 2002, Amazon Web Services (AWS) was founded by Amazon to provide data storing and computing services. Around the year 2009, big corporate giants for example Microsoft, Google, Oracle, and HP began to make offers related to services of cloud computing. In the modern era, almost every person makes use of services related to cloud computing in their daily routines like Google's drive, mail and photos, and Apple's iCloud, to consider a few. Cloud computing services are becoming a necessary need for the IT industry at the present time [5, 6].

Cloud computing has three components which are, 1) the client's personal computer allows the end-user to keep interacting with the cloud. 2) Servers are dispersed throughout the globe, yet they appear to be in communication with one another. 3) A data center is a collection of servers [3]. The characteristics of cloud computing have been illustrated in Fig. 1. These features of cloud computing give better understanding of it to users. These features are described as follows:

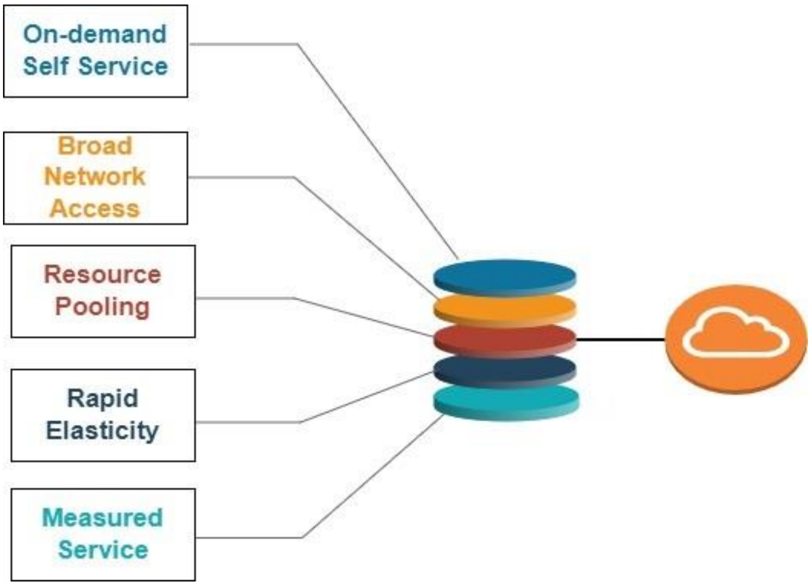


Fig.1. Characteristics of cloud computing

2.1. On-Demand Self-Service

Any dedicated system administrator is not required to continuously look-after the cloud computing services, consumers may provide, manage and monitor system processing power, memory and storage resources as required [11].

2.2. Broad Network Access

Broad network access and traditional networks are frequently used to provide computing services [11]. Broad Networks in Cloud Computing allow users to connect to a hardware network without having to pay for hardware configurations and maintenance, something that can be an expensive expense for companies. With Broad Networks, organizations can more efficiently manage IT costs by moving network configuration out of the data center and into specialized equipment that enables mobile users to connect to an organization’s central enterprise cloud services.

2.3. Resource pooling

It is a fundamental concept that allows for the efficient and cost-effective allocation of resources such as computing power, storage, and network bandwidth. This allows customers to only pay for the resources they actually use, rather than having to provision and maintain their own physical infrastructure. Uncommitted sharing of IT resources (e.g., servers, services, storage, networks and applications) between many occupants and applications. The amount of physical resources is the same amongst several clients [11].

2.4. Rapid elasticity

As per the requirement of clients or consumers the computing or IT resources should be able to scale in or out when needed in this type of computing services. The computing resource services should be scale up whenever any user requests services and when client has terminated his/her job then the services is scale down [11].

2.5. Measured service

For each service holder and application, a complete recorded file of used resources is stored which provides the clear image to the resources provider and consumer of an account of what has been used.This recorded file is used for resource management, usage, invoicing and for many other purposes [11].

3. SERVICE MODELS OF CLOUD COMPUTING

There are three cloud service models available in cloud computing. The goals of these different models are to fulfill the requirements of a different set of businesses. The three models included are Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS).

3.1. PLATFORM AS A SERVICE (PaaS)

In Platform as a Service (PaaS), users or programmers are provided with a platform and development environment as a service, giving them the ability to deploy, design, test, execute, and manage their software applications and codes. The users are not bound to build their software or applications to work on the provider's infrastructure. The features of PaaS are: 1) the same development applications can be accessed by multiple users, 2) the integration of databases and web services, 3) the computing resources should be able to "Auto-scale" when needed, 4) it should have the ability to support a variety of frameworks and multiple languages, 5) to meet the requirements of the firm, computing resources may be scaled down and scale up with the use of available virtualization technology. AWS Elastic Beanstalk, Force.com, Windows Azure, Google App Engine, Heroku, Apache Stratos, OpenShift, and Magento Commerce Cloud are examples of the Platform as a service (PaaS) [12].

3.2. SOFTWARE AS A SERVICE (SaaS)

The SaaS is also term as "On-demand software". In this type of service, a third-party cloud service provider offers the applications. Clients can avail these services by the use of an active internet connection and a web browser. SaaS is a method of delivering software, storage, and applications as a service through the internet. The consumer can access these services from anywhere, any place, and anytime rather than through machine installation. It removes any bounds of users with complex software and hardware. SaaS users do not have to buy, do maintenance, or upgrade their software or hardware [12].

The following are the features of SaaS: 1) controlled from a single place, 2) a remote server hosts the website, 3) available via the internet, 4) hardware and software upgrades are not the responsibility of users, 5) updates are implemented automatically, 6) pay-per-use services are available for purchase. Google Apps, BigCommerce, Dropbox, Salesforce, Cisco WebEx, ZenDesk, GoToMeeting, Slack, and other comparable services are some the examples.

3.3. INFRASTRUCTURE AS A SERVICE (IaaS)

IaaS gives many computing resources depending on the demand that includes storage, hardware, operating system (OS), and devices. IaaS is also term as “Hardware as a Service (HaaS)”. This infrastructure of computing is managed through the internet. The main focus of adopting IaaS is that it secures clients' time, money, and efforts because it removes the barriers of purchasing, managing, and monitoring physical servers. Through the use of an internet connection, IaaS consumers can access the services [12].

The features of the IaaS are 1) on the basis subscription resources are offered, 2) the services are extremely scalable, 3) access through a dynamic and flexible GUI and API, and 4) administrative tasks are automated. Examples of IaaS are Amazon Web Services (AWS), Linode, Microsoft Azure, Digital Ocean, Rackspace, Google Compute Engine (GCE), and Cisco Metacloud.

4. DEPLOYMENT MODELS OF CLOUD COMPUTING

The PaaS, SaaS, and IaaS are well-known service models amongst both clients and suppliers. To make use of cloud computing characteristics, these services can be implementing with the help of different deployment models, including private cloud, public cloud, hybrid cloud, and community cloud. The following are descriptions of each of these deployment models [4].

4.1. PUBLIC CLOUD

It is a form of cloud hosting in which cloud services are provided via a public network. An accurate representation of cloud hosting can be found in this model. Various clients receive services and infrastructure from the service provider in this cloud model. There is no influence on the location of infrastructure on the part of customers. Aside from security provided to public cloud users by cloud hosting providers, there may be little or no difference between public and private cloud architectures.

Businesses that need to manage their load will benefit from the public cloud. As a result of lower capital and operating costs, the public cloud is the most cost-effective option. Over the public internet, the public cloud is a computing service given by 3rd-party providers. Any consumer who wants to use these services can easily use them. Vendors may provide a service for free or a pay-per-use license policy. In the public cloud, the expense is shared by all users. Customers benefit because economies of scale are obtained. Google Cloud is an example of a public cloud that is offered for free [4].

4.2. PRIVATE CLOUD

The computing services, which are given by private network providers, are named private cloud, and these are exclusively available services and are not available to the public generally. An internal cloud is another name for it. This cloud computing platform is protected by a firewall managed by an organization's IT department and constructed on something like a secure cloud-based environment. Only approved users may access the private cloud, giving the organization greater control over its data. A distinct pool of physical computers, which may be located within or outside, provides resources to private cloud services. Organizations with unforeseen or changing demands, projects with critical management demands, and uptime requirements are better suited for the private cloud. In contrast to a public cloud system, a private cloud environment has no bandwidth restrictions or security requirements. A private cloud guarantees a significantly better level of privacy and security through internal hosting and a firewall. Since clients' accessibility and the networks they use are restricted, cloud providers have control over the infrastructure and increased security. Eucalyptus Systems is a good example [4].

4.3. HYBRID CLOUD

A hybrid cloud term refers to a system that makes a combination of public, private clouds, and community clouds. There can be two or even more clouds in this deployment model. These comprising of different clouds (cloud combinations such as ' public and private,' ' community and public,' and so on), but they are linked by preparatory technology or standardized that allows for data portability and application [13]. The hybrid cloud approach may be used by businesses to process large amounts of data. Scalability, flexibility, and security are all advantages of hybrid cloud hosting. Each cloud that is a hybrid cloud can be independently controlled, and the applications and data can be exchangeable among the clouds.

4.4. COMMUNITY CLOUD

This type of cloud model is shared by various firms, which deliver services to deal with common problems in a particular community. This can be controlled by an organization or a third party, and it can be deployed either off-site or on-site [13]. Because the expense is shared by certain organizations within the community, the community cloud can save money. Cloud hosting has become more popular among businesses.

5. SECURITY FACTORS IN CLOUD COMPUTING

Although cloud computing is surrounded by so many technologies, such as load balancing, concurrency control, networking, operating system, memory management, virtualization, database, and so on, various significant aspects might impact its performance[14].

These technologies' security factors affecting cloud computing are suitable, for example, the network that links cloud computing to the outside world must be protected. When mapping with physical systems, the virtualization idea must be carried out safely [15]. Load balancing is the process of managing incoming request traffic, which might cause the server to become overloaded. Malicious assaults can be mitigated using data mining methods.

According to Gartner [16], an American information technology research and consultancy business, cloud computing for service-enabled applications is still seven years away from market maturity. Scalability, interoperability, shared environment, and security are just a few of the issues it has faced thus far, not to mention other business-related issues. Cloud resources are virtualized, and diverse cloud service customers use the same infrastructure and platform for developing applications and storing data. Architecture set, asset alienation, and data isolation are three significant areas of interest. Any violent or unauthorized access to a cloud service user's private information runs the risk of compromising its accuracy, confidentiality, and privacy.

5.1. Cloud threats

Several risks were examined throughout time, and it was discovered that thefts and unauthorized access had compromised a considerable quantity of data. Other security threats included loss, combination, IT disasters, improper disposal, and so on [17].

5.2. Security

"How information can be locked safely?" is how security is defined. The fact that sensitive business data would be stored outside thecompany's firewall raises serious issues. If adequate precautions are not followed, a great deal of very sensitive information might be made public. Even if only one site is hacked, hacking and other assaults on cloud infrastructure will affect several clients. Using security apps, encrypted data file schemes, data loss software, and acquiring security hardware to track out of the way behavior across servers helps reduce these dangers [15].

5.3. Distributed Responsibilities

The primary security concern is, the user must double-check before transferring sensitive data to cloud storage. They must also take reasonable security precautions, such as encrypting data with 32-bit encryption. It is an important step because data may be protected if it is encrypted before being saved on the cloud. As a result, even if an intrusion occurs, the risk of data theft is extremelylow. The diagram below illustrates cloudencryption.

5.4. Fault tolerance and failure recovery

The data center's primary duty is to process massiveamounts of data every day. Due to a breakdown ofthe cloud infrastructure, cloud services may experience data loss. The breakdown might becaused by a lack of power, a lack of room, or a failure of the primary system.

6. CHALLENGES FOR CLOUD COMPUTING

Cloud computing has become so popular in recentyears that it is now at the forefront. Along with itsmany advantages, cloud computing has several security challenges that require immediate attention to improve the service [18]. Fig. 2 shows the cloud computing challenges and these have been explained in detail.

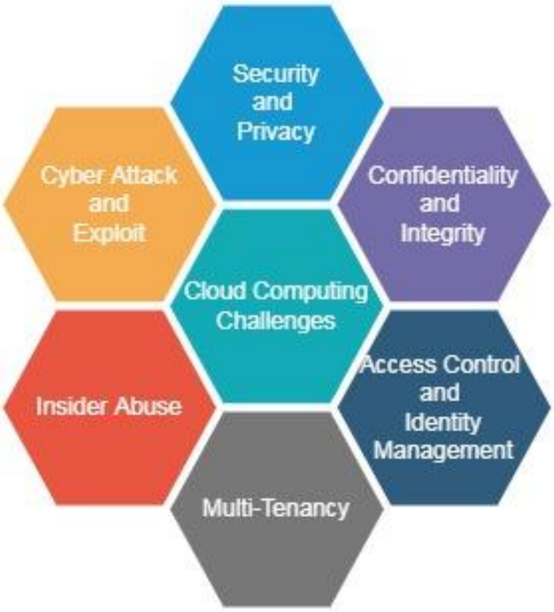

Security and Privacy
Cyber Attack and Exploit
Confidentiality and Integrity
Cloud Computing Challenges
Insider Abuse
Access Control and Identity Management
Multi-Tenancy

Fig.2. Security challenges for cloud computing

6.1. Outsourcing

When data is outsourced, the customer may lose control. To prohibit cloud service providers (CSPs) from using data without their clients' consent, some form of acceptablemethod is required.

6.2. Multi-tenancy

Cloud computing is a shared pool of resources. When offering a multi-tenant environment, data protection must be considered.

6.3. Service Level Agreements (SLAs)

A written agreement between the consumer and the supplier is required. The primary purpose of these agreements is to take all necessary steps.

6.4. Heterogeneity

Different cloud providers have a variety of data protection mechanisms, which makes integration difficult.

6.5. Server Downtime

Downtime is the amount of time it takes for the system to respond to a client after a service failure. Downtime should be avoided as much as possible, and power backups should be established.

6.6. Backup

Client data should be backed up in case of a service failure. The Cloud Seller should specify in SLAs how to address these issues in the event of a disaster. The likelihood of a total system breakdown as a result of major catastrophes, such as flooding, earthquakes, and so forth, is incredibly low.

6.7. Data Redundancy

Data redundancy occurs whenthe same data is stored in two separate locations. Cloud computing may be defined as providing customers with copies of the same data, systems, or equipment. Data redundancy should be kept to a minimum by cloud sellers.

6.8. Data handled by a third party

Because data in the cloud is handled and controlled by a third party, the largest issue is determining the security measures the party employs and what assurances the data is secure because no third party can guarantee 100 percent data protection. As a result,data security cannot be guaranteed.

6.9. Cyber-Attack

Cyber Attack is one of the most serious security threats in cloud computing. Different sorts of data breaches are carried out, ranging from malware and ransomware to simplemisconfigurations or poorly created infrastructures [19]. There are several issues, and when it comes to malware, we are witnessing that it is becoming increasingly polymorphic, attacking various routes at the same time [20]. Becauseit's meant to spread so quickly, having a handle onit requires a new perspective on cloud security.

6.10. Insider Threat

Assume that the cloud firm where you have saved your data has users who may readily access the data, which implies the data will not be private.

6.11. Government Interference

Different sorts of surveillance and monitoring program are used by governments to monitor data. As a result, you can never claim that your data is only accessible by you. Different authorities have access to your data, hence there is no data privacy.

6.12. Lack of Service

There is no sufficient support from firms to their users since there is a lot of rivalry in the market, therefore a company cuttheir data storage pricing to compete, which leads to a lack of support for clients.

6.13. Standardization Lacking

Different cloud providers do not necessarily adhere to the sameset of guidelines. That implies there are no adequate standards in place for various technologies such as encryption, authentication, oraccess control.

6.14. Integrity of Data

There is always the possibility of data being modified by an unauthorized user. Essentially, it is the responsibility of the Cloud Service Provider to ensure that data is not altered by an unauthorized user [21]. When data is transported from one cloud to another, the second idea of integrity comes into play. As a result, the Cloud Service Provider must ensure that data is not altered by an unauthorized person at that point and transparency is lacking.

When a company purchases a public, private, or hybrid cloud service from a cloud service provider, they aren't given the specifics on how their data will be protected. This is due to a lack of service transparency, making it impossible for businesses to determine if the data is kept and processed is truly safe [22, 23]. People are unsurewhether or not their personal information is safe.

6.15. IP Spoofing

Analysis of data being transferred across the network is known as IP Spoofing. The attacker manipulates data as it is transferred over the network. The manipulation is carried out in such a manner that the trusted system's IP address is used to modify the packet information before sending it to the receiving system.

6.16. DDOS Attack

In a DDOS attack, the attacker spoofs information and makes a large number of data requests. The server becomes confused and unsure what to do with all of these requests, eventually releasing authorized data.

7. SOLUTIONS FOR SECURITY PROBLEMS OF CLOUD COMPUTING

Cloud computing security issues must be properly addressed. Adopting the cloud environment becomes more challenging if proper solutions are not given [14]. Aside from adoption, data transmission and operation are becoming increasingly laborious. The data security and privacy are the most important factors for all [24]. Because the cloud is a common pool of resources, the main security concern is data leakage and data separation. The next more difficult task is to prevent data leaking. To address the above-mentioned issues, the following are some ideas to consider whileaddressing cloud computing security issues.

Data Encryption: Data encryption in the cloud is the process of transforming or encoding data before it is transferred to cloud storage [14]. Data encryption is the process of encoding data into a hashed version. It serves to reduce the threat of unauthorized access to that data by unauthorized persons or processes. A good cloud-based data encryption feature can significantly increase business productivity and security in offsite storage.

Access controls: Cloud providers can implement access controls to ensure that only authorized users can access data stored in the cloud.

Multi-factor authentication: This can be used to ensure that only authorized users can access data stored in the cloud.

Virtual private networks (VPNs): VPNs can be used to secure communications between a user's device and the cloud.

Firewalls: Cloud providers can use firewalls to protect their networks from malicious traffic.

Regular security audits: Regular security audits can be used to identify and address any security vulnerabilities in the cloud.

Compliance with industry standards: Cloud providers should comply with industry standards such as SOC 2, PCI DSS, and HIPAA to ensure that they are adhering to best practices for security.

Use of reliable cloud providers: Choosing a reliable and reputed cloud provider can help ensure that your data is stored securely.

Digital Signature: It is a cryptographic method which used to check the authorization and authentication of the data. Two separate operations are done by the digital signature: 1) a signing key is not required for a signing operation, and 2) a signing key is imposing by the signing operation that establishes a signature over raw data.

It is important to note that security in cloud computing is a shared responsibility between the cloud provider and the user. The user must also ensure that they are following best practices for security, such as using strong passwords and keeping their devices up to date with the latest security patches.

8. BENEFITS OF CLOUD COMPUTING

Cloud computing provides a list of benefits to its users. Some of them are enhanced security of data, scalability, flexibility, cost saving and many others.

Enhanced Security: To guarantee excellent security key distribution, data encryption, tight access controls, and security intelligence are all used in cloud computing [17]. It provides extra layers of protection for user sensitive data and data-at-rest. This helps service providers to increase user productivity, prevent denial of service (DoS) attacks, deal with malware, and much more.

Cost Saving: Cloud computing consumers must only pay for the services they make use of. Maintenance costs are found low because the infrastructure is not bought by the consumer.

Flexibility: A feature of cloud computing scalability is very crucial because the quick scaling up and down of your co-operations may swift necessary adjustments to resources and technology, cloud computing gives flexibility to manage these varieties.

9. CONCLUSION

Cloud computing is a relatively new technology that is rapidly gaining popularity. This paper provided an overview of cloud computing, including its multiple security elements and significant factors that affect cloud security. Cloudcomputing has great potential, but the security risks associated with it are equally proportional to the benefits it provides. Cloud computing is a good potential and profitable choice for both corporations and attackers, both may benefit fromit. Both the user and the supplier of cloud services should ensure that their cloud is completely protected. Cloud computing is gaining popularity in every business, but it is troubled by security and privacy concerns, which are preventing broad use. As a result, every company should have dependable security procedures in place to employ technology to secure customer data. While many clouds contain firewalls and intrusion prevention systems, they are not suited to the client's specific needs. To be able to do the appropriate things to defend our networks, we need a clear and more consolidated approach. Solutions to these issues have been proposed, which may be used to improve cloud service.

Acknowledgment

The authors wish to thank Sindh Madressatul Islam University for the acceptance of our work for publication.

References

[1] Qian, L., Luo, Z., Du, Y., Guo, L. (2009). Cloud Computing: An Overview. In: Jaatun, M.G., Zhao, G., Rong, C. (eds) Cloud Computing. CloudCom 2009. Lecture Notes in Computer Science, vol 5931. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-10665-1_63

[2] Wang, L., von Laszewski, G., Younge, A. et al. Cloud Computing: a Perspective Study. New Gener. Comput. 28, 137–146 (2010). https://doi.org/10.1007/s00354-008-0081-5

[3] Mathew, S., Gulia, S., Singh, V. and Dev, V., 2017. A Review Paper on Cloud Computing and Its Security Concerns. RICE, pp.245-250.

[4] Jathanna, R. and Jagli, D., 2017. Cloud computing and security issues. International Journal of Engineering Research and Applications, 7(6), pp.31-38.

[5] Sabir, Sabiyyah. "Security issues in cloud computing and their solutions: a review." *International Journal of Advanced Computer Science and Applications* 9.11 (2018).

[6] Kumar, Rakesh, and Rinkaj Goyal. "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey." *Computer Science Review* 33 (2019): 1-48.

[7] Che, J., Duan, Y., Zhang, T. and Fan, J., 2011. Study on the security models and strategies of cloud computing. Procedia Engineering, 23, pp.586-593.

[8] Waqas, M, Kumar, K, Laghari, AA, et al. Botnet attack detection in Internet of Things devices over cloud environment via machine learning. Concurrency Computat Pract Exper. 2022; 34(4):e6662. doi:10.1002/cpe.6662.

[9] Knight, S., 2020. Strategies to Reduce Small Business Data Security Breaches (Doctoral dissertation, Walden University).

[10] Shackelford, S.J., 2012. Should your firm invest in cyber risk insurance?. Business Horizons, 55(4), pp.349-356.

[11] Al-Issa, Yazan, Mohammad Ashraf Ottom, and Ahmed Tamrawi. "eHealth cloud security challenges: a survey." *Journal of healthcare engineering* 2019 (2019).

[12] Abdulsalam, Yunusa Simpa, and Mustapha Hedabou. "Security and privacy in cloud computing: technical review." *Future Internet* 14.1 (2022): 11.

[13] Bulusu, Santosh, and Kalyan Sudia. "A study on cloud computing security challenges." (2013).

[14] Qadiree, J. and Maqbool, I.M., 2016. Solutions of Cloud Computing Security Issues. International Journal of Computer Science Trends and Technology (IJCST), 4(2), pp.38-42.

[15] Shirvani, Mirsaeid Hosseini, Amir Masoud Rahmani, and Amir Sahafi. "A survey study on virtual machine migration and server consolidation techniques in DVFS-enabled cloud datacenter: Taxonomy and challenges." Journal of King Saud University-Computer and Information Sciences 32.3 (2020): 267-286.

[16] Gartenr Inc.,"Gartner Says IT Organizations Will Spend More Money on Private Cloud Computing Investments Than on Offerings From Public Cloud Providers Through 2012" ,http://www.gartner.com/it/page.jsp?id=1239813, December 1, 2009.

[17] Mell, P. and Grance, T., 2011. The NIST definition of cloud computing.

[18] Shahzad, F., 2014. State-of-the-art survey on cloud computing security challenges, approaches and solutions. Procedia Computer Science, 37, pp.357-362.

[19] Tadapaneni, Narendra Rao. "Different Types of Cloud Service Models." (2017).

[20] Waqas, Muhammad & Khuhro, Mansoor & Saeed, Umair & Kumar, Kamlesh & Mirbahar, Naadiya & Rajab Khan, Ruqiya. (2021). Security Awareness on Ransomware Threats Detection and their Protection Techniques. International Journal of Advanced Trends in Computer Science and Engineering. 10. 975 – 983.

[21] Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), pp.9493-9532.

[22] Milkaite, I. and Lievens, E., 2020. Child-friendly transparency of data processing in the EU: from legal requirements to platform policies. Journal of Children and Media, 14(1), pp.5-21.

[23] Winkler, Vic JR. *Securing the Cloud: Cloud computer Security techniques and tactics*. Elsevier, 2011.

[24] Martin, H., Ma, Z., Schmittner, C., Winkler, B., Krammer, M., Schneider, D., Amorim, T., Macher, G. and Kreiner, C., 2020. Combined automotive safety and security pattern engineering approach. Reliability Engineering & System Safety, 198, p.106773.

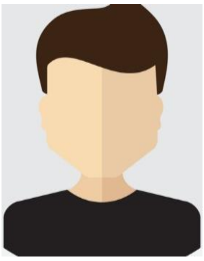
Authors' Profiles

Tahir Muzaffar is currently a student at computer science and working as an internee at 8Technologist Karachi Pakistan.

Ushna Ali is currently a student at computer science and working as an internee at National Incubation NEP NIC Karachi, Pakistan

Muhammad Waqas completed his B.E in Telecommunication from Sukkur IBA University. He is working as an Assistant Network Engineer in a project based job at Karachi, Pakistan. His research interests include the AI systems, Machine Learning, Deep Learning and Network Security.

Muhammad Shahbaz is currently a student at computer science and working as an internee at National Incubation NEP NIC Karachi, Pakistan



Moiz Khan is currently a student at computer science and working as an internee at 8Technologist Karachi Pakistan.

Usama Khan is currently a student at computer science and working as an internee at National Incubation NEP NIC Karachi, Pakistan