I.J. Information Engineering and Electronic Business, 2021, 3, 30-38
Published Online June 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2021.03.04

A Review of Data Security Challenges and their Solutions in Cloud Computing

Isma Zulifqar[1], Sadia Anayat[2], Imtiaz Kharal
[1,2]Govt College Women University Sialkot, Pakistan
Email: cssadiaanayat@gmail.com

Received: 12 August 2020; Accepted: 17 November 2020; Published: 08 June 2021

Abstract: Cloud computing is the newest web based computing network that offers the users with convenient and flexible resources to access or function with different cloud applications. Cloud computing is the availability of the computer network services, mainly storing data and computational power, without explicit user active control. The data in cloud computing is stored and accessed on a distant server by using cloud service provider' applications. Providing protection is a main issue because information is transferred to the remote server through a medium. It is important to tackle the security issues of cloud computing before implementing it in an organization. In this paper, we call attention to the data related security issues and solution to be addressed in the cloud computing network. To protect our data from malicious users we can implement encryption. We have discussed the advantages of cloud computing in our paper.

Index Terms: Cloud computing, data security, E-waste.

1. Introduction

Cloud computing is the newest web based computing network that offers users with convenient and flexible resources to access or function with different cloud applications. The internet is the leading force for the different technologies which have been developed. Cloud computing is one of those that has been addressed lately. It is an enumerated standard [1] for linking a large pool of shared or private system to offer the flexible implementation, facts, figour and information storage infrastructure. Cloud computing is a realistic way of realizing unmistakable cost advantages and this has the potential to turn a data center from a large-exhaustive enviroment into a variable price setting [2]. Cloud computing has appeared as the new technology that has been evolved over the past few years and in the years to come has been considered the next big issue. As it's a latest technology, it require latest security vulnerabilities and it also faces different issues [3].

The cloud computing model has moved significantly and exponentially towards its development, and it has become a revolutionary phenomenon in information technology as it offers its consumers and providers substantial cost savings and new business opportunities. Cloud computing is defined by customers who used cloud services as desired, who utilize pooled resources as a service that can grow high or low as wanted quickly and elastically, who pay only for what is being used and who access services through a networked infrastructure. Cloud infrastructure is changing the traditional services IT delivery model. Company and IT results include cost-reduction, scalability, efficiency, asset usage, improved efficiencies and mobility [2]. Vendors of cloud computing services praised the security and performance of their services, the cloud computing actaul delivery is not as secure and reliable as they say.

Cloud computing offers a way for cloud data to be stored and accessed remoutely by linking the cloud app to the internet [4]. Customers will be able to save their Meta data in the cloud data server by selecting the cloud services [5]. The information stored in the cloud data center can be retrieved or handled by cloud service vendors. The data collected for data processing in a cloud data center should therefore be performed with utmost professionalism.

Data in a cloud requires its own protection, particularly data separation in the cloud service to secure data. Data separation can be accomplished to different levels by virtualization, encryption and authentication. That enhances data security from unauthorized person [10]. It is important when it comes to joint accupation cloud setting that can have many clients or clients who neither see nor exchange the data with each other but can share resources or software in an implementation setting, even though they may not adhere to the same enterprise. Agencies are now seeking to avoid having to concentrate on the IT structure. To increasing the productivity, they need to concentrate on their business operation. The cloud computing has many possible benefits as opposed to the conventional IT model. However, from the user viewpoint, questions about cloud computing protection exists a major obstacle to cloud computing acceptance. Cloud computing is the availability of the computer network services, mainly storing data and computational power, without explicit user active control. Cloud data are processed and retrieved on a web server, using cloud service vendors services. The value of

cloud computing is therefore growing, to become a growing market and attraction a great deal of attention from the educational and business sectors. Cloud storage system sadly suffered from many issues, such as lack of access and security concerns. Cloud computing security concerns: honesty, integrity, availability, verification, permission, and confidentiality because the cloud storage service is focused on two way sharing of data between service provider and customer. Consequently, the chance of compromising data is increasing and can be divide into two major groups: essential data and archival data. Important information is the information that a subscriber needs at any moment and any pause or disappearance would annoy him. Moreover, the archival data is the data that collectively very rare, often at a non-critical time. Therefore, gap in it won't be able to be considered as the key problem.

Structure

This paper is structures as follow: the introduction of LCoud Computing has been given in section 1 and background is discusses in senction 2. Then, the related work is provided in section 3 and challenges are given in section 4. Moreover, the types of cloud computing are discussed in section 5 and advantages of CC are given in section 6. the discussion is provided in section 7 and conclusion is drwan at last in section 8.

2. Background

Indeed the word may have been used in Compaq a year earlier. The emergence of cloud computing is a very new tendency white its origin refers with new industry, technological and environmental insights to a certain outdated ideas. Cloud computing in the 1950s is the concept of the idea of the "time sharing" from which multiple people would share rights to content and processing power. The word was conceived in a 1997 discussion on a "modern computing model" by University of Texas professor Ramnath Chellapa. Back in the 1960 John McCarthy presented the idea of cloud computing. As per him, computing "can be structured as a public resource soon".

In 1966, Douglas Parkhill first discussed the features of cloud computing in his book "The question of the machine utility". in this study, the different features and issued related to data security are discussed. Popovi and hocenski addressed safety concerns, specifications and issues that cloud service supplier in cloud engineering need to answere. Then in 1969 J.C.R Licklider, whose dream was to interconnect all across the world and to control services and content at every location, created the ARPANET from anywhere-the router which became the web's base. Origin of the word "internet" originates from the world of telecommunications, where telecommunications organizations began providing VPN services along with similar service quality at somewhat cheaper cost. They established specialized point-to-point data cables since invention of VPN that are nothing more than bandwidth inefficiency. However, they are able to change traffic to match network performance efficiency by using VPN services. It has now expanded by cloud computing to include databases and network infrastructure. Many business companies have moved into, and introduced cloud computing. Amazon held a significant role for example and introduced the Amazon Web Services in 2006. Google and IBM have both begun research projects in cloud computing alongside this. Eucalyptus is the first open source, private cloud deployment platform.

In 1999, salesforce.com launched one of the first functional clouds computing applications and set out the idea of offering enterprise services via a website.

In 2002, via the Amazon electronic Turk, Amazon Web Services introduced a cloud-based suite of products involving space, networking and indeed human intelligence. This achievement has prefaced by its flexible computing web service in 2006 that offers a commercial operation by which customers can hire devices and execute their own programs. Google released the functionality of Google docs of that year. Google Docs has initially based on Google Spreadsheets and Written, two different ingredients. Google acquired Writely , which provides tenants the freedom to copy, modify and moved documents through blogging schemes. Google Spreadsheets (obtained in 2005 from 2 web innovations) is a web-based software that allows users to create, upgrade and modify and exchange information online. Ajax based applications, compliant with Microsoft Excel, is used. Save the spreadsheets as HTML format.

In 2006, AT & T also joined the cloud-computing field when USinter-networking was needed. USI was a software platform with applications in more than 30 states. AT & T launched synaptic in 2008, that merged the five USi internet data bases in the USA, Europe and Asia to act as a global portal under its cloud. IBM launched the IBM intelligence cloud platform in 2011, in help of faster cloud. Apple then released the ICloud, which aims to store more personally identifiable information (images, videos audios etc). in this year, Microsoft has began promoting the cloud on television, telling the general public of its potential to save images or video with convenient access.

Oracle launched the Oracle cloud in 2012, providing the three core business components (IaaS, PaaS and SaaS).

Web 2.0, Google, Yahoo, Microsoft and other internet providers currently support software based business technology applications is the ultimately example of cloud technology today.

Now that cloud computing has developed as a feasible and readily accessible resource, several people from diverse backgrounds (financial organizational, students and hackers) use virtual computers to carry out their daily routines. In order to ensure efficiency, this climate needs an implicit degree of awareness.

3. Related Work

Cloud data security is a big issue and different methodologies are proposed [6], also enhancing data security risk assessments in cloud computing [7], growing concerns about data storage problems related to privacy [8], so that no private data can be retrieved as in the case of hacked emails data security. the following are the studies in which different researchers addressed the data secuirty challenges and their possible solution in cloud computing.

Popovi and hocenski addressed safety concerns, specifications and issues that cloud service supplier in cloud engineering need toanswere [16].

Maggi and Zanero discussed countermeasures built to reduce well-known threats to defense. The key emphasis is on outlier-based solutions that are most suitable for current security systems and not for sensors of intrusions. Improvements in pattern are observed.

Md. Tanzim Khorshed et al [18] claims that cloud technology manages to cut service costs and boost business performance. Yet there are also security issues to be tackled to promote this and promote its use by the IT consumer sector. They also noted that online services provide an enticy target for cyber threats and illegal activity as these platforms have data stored in their databases from many companies and individuals. The analyst conducts a cloud-computing questionnaire to identify vulnerabilities and security issues and list five rising kinds of attacks 1: Denial of service 2: Molevolent intruder attacks 3: Workstation side network attack 4: phishing attacks 5: shared memory target attacks. They suggested a framework automatically classify such threats and checked their efficiency by visualizing threats in a specific cloud environment.

A report by Farhan Bashir Sheikh et al in [19] incorporates information from eleven publications regarding vulnerable security threats. The researchers computed their results i.e. the topic examined and the methodology used in their document to resolve the issue.

In [20], Eystein Mathisen addresses several primary security concerns related to cloud computing and strategies used to minimize the risk. The researcher claims that cloud-computing use will expand in the coming years and more business will exchange their data with multiple servers that could generate massive groups of attackers. He often claims there are prospects for interoperability and data lock in problems in the future, which can be minimized by using open source software from the time of cloud computing implementation.

Ertaul et al., listed the attributes of CC such as minimized cost of maintenance, scalability and market divergence. They believe cloud computing also reduces sophistication and offers consumers with quicker and simpler service implementation. The strategy used to interact with service quality is virtualization. This also addresses the benefits of applying CC from a particular agenda. They also suggested that certain regulations are needed in CC [21].

Wentao Liu implemented some cloud computing platforms and examines security concerns in cloud computing and its approach as per the principles of the cloud computing [22].

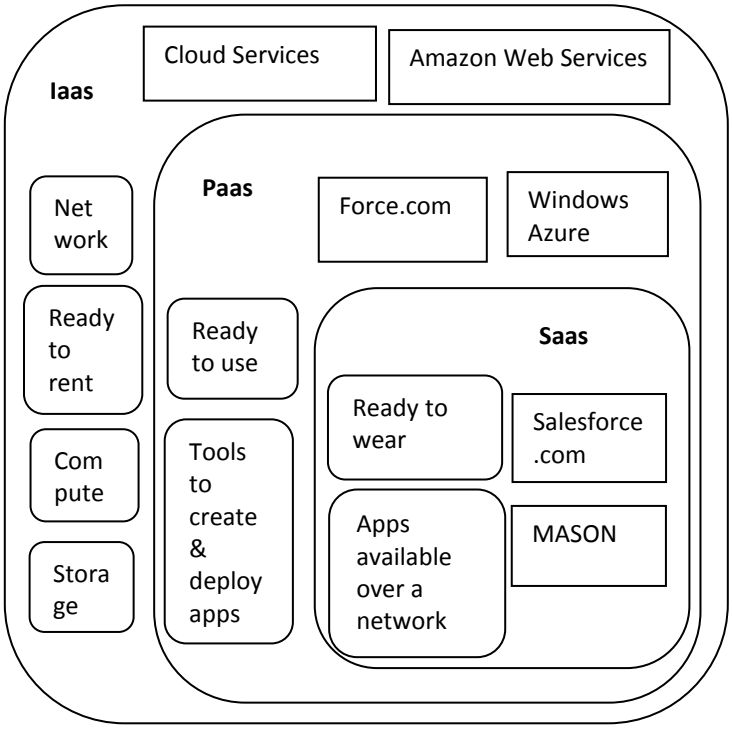


Fig.1. Types of Cloud computing[23]

Mohamed E.M et.al introduced cloud computing data protection structure based on a cloud architecture report. We also introduced tools to improve the cloud-computing job in the data protection model [23].

We have identifies various difficulties in cloud computing here in this section. When we use the internet-cloud platform, data protection and privacy need to be strongly emphasized. Information loss or data exposure can

4. Challenges to Cloud Computing

We have identifies various difficulties related to security of data in cloud computing here in this section. When we use the internet-cloud platform, data protection and privacy need to be strongly emphasized. Information loss or data exposure can seriously affect a company's reputation and confidence. Prevention of data leakage is regarded to be the most critical problem with 88% of major challenges. Likewise, data remoteness and privacy impact security problems by 92%. Cloud computing most critical security concerns are: data protection, reliability, honesty, availability, authentication an confidentiality, lack of resources and skills etc. data lie cycle has six phases Build inventory, Use, Transfer, Archive and Kill.

4.1 Integrity:

Data on the cloud can be impacted by the damage caused by transmitting data to cloud storage [25]. Since the information and calcultion are subcontracted to a web server, the validity of the data should be continuously protected and viewed to ensure information and calculation are interact. Data integrity means that records are secured from unlawful alternation. Some modifications to the details need to be observed.

4.2 Availability:

Accessibility refers to the cloud subscriber's ability to obtain the necessary data at any time [26]. One major issue for each company is whether they can retain access to cloud computing resources at any time. When an approved person may use and control the device and save data at any moment, a system is call available. Service provider will also confirm that the information available is accessible to customers from various places at any time.

4.3 vender lock in:

Business entities that use cloud-based services often that decide to change their Cloud Service Provider (CSP) and switch to a new one. This may be due to some excuse because the CSP will no more adapt to the tenant's need, whether there are improvements or upgrades in the services that are not expected by the customer. Because they are unable to satisfy the needs to customers or any other trigger that makes the customer switch to a new CSP but they cannot get out of this condition, which is known as Vender Lock-in condition.

4.4 Data security:

It is important to give the encryption, certification and intrusion detection for information saved in the cloud to improve the safety in cloud computing. Particular state, the data is spread across tmultiple of areas in cloud computing. It is hard to find the data. Unless the data is transfer to various geographical areas, the data laws can also alter.

4.5 Interoperability:

Thats the willingness of two or more processes to work with each other to share data and to use it [28]. Failure to integrate these systems makes it impossible for companies to incorporate their infromation technology network in the cloud to achieve efficiency gains and cost savings. There are also cloud-computing networks that are built as closed systems, so they are not built to connect.

Table 1. Challenges of Cloud Computing

Sr. No	Challenges	Model	Description	significance	Limitations/F.W
1	Data availability	service provider agreement framework	SLA parameters and flexible negotiation methods	Manage the appropriate emergency response and plan and unplanned	Needed complex computation.should provide high protection mechanisms
2	Data Storage	Data storage framework PaaS	combine and extend multiple databases and.	user centric trust model to help users to manage the storage	Need less time.
3	Integrity	MAC algorithms.	The owner of data must Import the outsourced data and and then measure	Unplanned and expected changes will be noted	Run on only client side.Should need to technique to detect attackers.
4	Security	Hidden Markov Model (HMM)	detect any type of security breach	identify security in cloud computing network.	sometimes employee cannot Use it.Should provide flexible modal

5	resource scheduling	skewness matrix	the capacities of servers are well utilized	Equally shared serviced between cloud users and provider of infractructure	Just consider user's priorities .Should need best measurement level.
6	Resource allocation(RA) in IaaS	optimize genetic algorithm with multifaceted	necessary to arrange and share on changeable demands	resources are consummate with the support of virtualization technology	Prioritization RA in relation is limited available resources
7	Translating high-level Quality of services objective into low level	J Meter	To produce large volume of test traffic required for quality of services matrics	one of the most popular load testing tools, requires	We should analyzed our needs to derive threading
8	absence of end-to-end test orchestration	QoS metrics.	A few QoS matrics to watch	Multipulation of several configurable low level data	Focusing the genration load only. In F.W we should provide more level of details
9	Resource bottleneck	QoS	Add switch to stronger CPU	Understand the accurate resource utilization status	Less excess capacity. work continue on QoS metrics
10	optimizing cloud resource	GROWL	generates an optimized resource configuration	Cover the load check data from from low level configuration and review.	Must GROWL enrich and show load testing activities.
11	To protect the data	cryptographic	Security of data stored in database	Backup data needed, tenacity storage unit	Transmission of very large documents is prohibitive.
12	authentication	two factor and multifactor authentication	migrating your system to the cloud	technologies come with vulnerabilities like Public Key Infrastructure solution	security proofing technique is on process,.
13	Legal and regulatory issues	data holding and legal finding.	trusted storage technique can play a key role	Regulatory compliance is when a company obeys the laws	Should awareness of laws in countries where your customers live
14	Lock-in	recognized the vendor lock-in problem	Discovered for enterprise adoption from a business	Just to avoid the bulky process.	Not all applications run. we will include implementation effects
15	Privacy and Security	The community understanding of privacy and protection	Massage data at the edge of the network.	Personal data may be extracted before processing	limitize number of people. opportunity for human error should be reduced

In table 1 we have explained different challenges of data security in cloud computing like vender lock in, availability, data security and integrity etc. And also we briefly explained the description of these.

We have also mentioned the proposed models of these challenges. Significance of these models are also very important and discussed the limitations of the proposed solutions too.

5. Types of Cloud Computing Security:

Categories of CC security, shown in Fig. 2, include: identity, information, infrastructure, network, and software security [29].

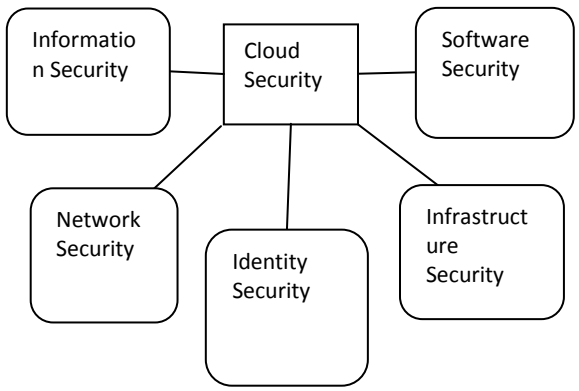


Fig. 2. Cloud Computing Security types

5.1 Identity Security:

It is described as the methodology of privacy and profession that " allows the authenticate people to retrieve the resources at the appropriatet time and for the good objectivess" [30]. It maintains data and apps privacy and security while enhancing their access to verified peoples.

5.2 information security:

Obligations for information protection include maintaining a collection of business operations that will safe data resources disregarding of whether the data has been encode or whether it is in transported, processed or deposited [31].

5.3 Network Security:

Network security is an essential computing prerequisite. It includes taking defensive hardware and software steps to prevent the existing networking infrastructure from unvarified persons, violation, breakdown, adjustment, degradation or inappropriate dissemination, thereby providing a stable forum for machines, clients and services to execute their vital functions throughout a safe environment [32]. Network level concerns can impact the web system specifically that essentially affects the capacity and increases device latency.

5.4 Software Security:

To establish a process of security analysis, security issues for applications should begin with the concept for the program and continue via the layout and execution processes. All of these steps rely on the other to offer the best software protection level [33]. Although there is a wide variety of an effort in the development of software in terms of complexity, they all need security guarantee.

5.5 Infrastructure Security:

To be able to check the business needs that the underlying infrastructure is safe and it is completely necessary for an enterprise. Elements need to be kept separate [34], too. Separating modules from management allows network users to avoid convenient access to memory drivers or cryptography codes.

5.6 Solutions:

Advanced encryption algorithm added to cloud computing to improve the security defense.

Encryption based on attribute, homomorphic encryption and symmetric encryption are the main types of encryption. Attribute encryption consists of either text security cipher or key code. This is used to clarify the encrypted texts as well as the secret numbers invoice encoded text that a client remains behind for decryption [35]. Using homomorphic encryption in CC enables for easy processing of the encrypted content. Symmetric encryption requires a rudimentary cryptography, which facilitates protected search capabilities over sensitive data. These forms of encryption can be enhanced with active products to ensure strong data security.

6. Advantages of Cloud Computing:

- Different advantages of cloud computing is as follows:
- Resilience
- Variation of Information technology
- Expand memory
- Superlative mobility
- Reduced cost

Such benefits of cloud computing attract much interest from the information and technology community. ITC reports in 2008- 2009 indicate that many businesses and individuals are finding that cloud computing is offering support in comparison with conventional computing methods [36].

7. Solution to Data Security Challenges

As a safer way to protected records, encryption is proposed. It is easier to store data in the cloud server until for encrypting files. Data Owner should grant permission to specific member of the community so that details can be readily accessible via them. To include data access control, heterogeneous data-centric authentication should be used. A blueprint for data protection it must be designed for authentication, data encryption and data integrity, data recovery, user protection, and improve the protection of data in the cloud. Data encryption should be used as a service to ensure privacy and data confidentiality. Apply encryption to data that makes data absolutely unusable and unusable to block access to data from other users. Accessibility can be complicated by standard encryption. Users are advised to review before uploading data to

the cloud if the data is stored on backup drives and the keywords remain unchanged in the files. Compute the hash of the file would ensure that the data is not changed until transferring it to cloud servers. It is possible to use this hash calculation for integrity of records, but it is very difficult to preserve it. Testing the integrity of RSA-based data can be done by merging identity based and RSA Signature cryptography. SaaS guarantees that all constraints must be transparent at the stage of the in order to segregate data from various participants, physical level and device level.Architecture for distributed access management may

It is used in cloud computing for access control. Usage of passwords or attribution to recognize unauthorized users policies that are centered are stronger. Permission as a service can be used to warn the customer that it is possible to access that part of the data. The fine grained access management scheme helps the owner to assign most computer-intensive functions to the cloud without revealing the data material, servers. For stable data collection, a data-driven architecture can be designed to and sharing with users of clouds. To track attacks in real-time, a network-based intrusion prevention framework is used.

Computing huge files of varying sizes and addressing the RSA-based storage security approach of remote data security can be used.

8. Prons and Cons of Cloud Computing

Cloud computing is the newest web based computing network that offers users with convenient and flexible resources to access or function with different cloud applications. Cloud computing offers a way for cloud data to be stored and accessed remotely by linking the cloud app to the internet [4]. Customers will be able to save their Meta data in the cloud data server by selecting the cloud services [5]. The information stored in the cloud data center can be retrieved or handled by cloud service vendors. The data collected for data processing in a cloud data center should therefore be performed with utmost professionalism. Cloud computing has such versatility, efficiency, usability and cost savings characteristics, which are very motivating. It is the latest emerging technology, which offers users many benefits; it faces many securities. The cloud computing has many possible benefits as opposed to the conventional IT model. However, from the user viewpoint, questions about cloud computing protection exists a major obstacle to cloud computing acceptance. Cloud computing is the availability of the computer network services, mainly storing data and computational power, without explicit user active control. Cloud data are processed and retrieved on a web server, using cloud service vendors services. The value of cloud computing is therefore growing, to become a growing market and attraction a great deal of attention from the educational and business sectors.

But we have to face a lot of problem while working with cloud comptuing. We have identifies various difficulties related to security of data in cloud computing here in this section. When we use the internet-cloud platform, data protection and privacy need to be strongly emphasized. Information loss or data exposure can seriously affect a company's reputation and confidence. Prevention of data leakage is regarded to be the most critical problem with 88% of major challenges. Likewise, data remoteness and privacy impact security problems by 92%. Cloud computing most critical security concerns are: data protection, reliability, honesty, availability, authentication an confidentiality, lack of resources and skills etc. data lie cycle has six phases Build inventory, Use, Transfer, Archive and Kill.

9. Discussion

Cloud based computing is one of the new trend which is emerging today, and ongoing search zone which has a positive subsequent. The users of this technology can control their resources whenever, all over the place. Cloud is seeing as a diligent and significant organization that has brought into the information technology sector. Consequently, the information technology sector demands to migrate to CC that involves consideration of many critical problems such as security. In addition, creativities need to incorporate CC to help them reduce costs and improve performance. We have spoken about the current problems here. Solutions must be reevaluates accurately as to their suitability for clouds. We sum up our obstacles very successfully with their constraints and suggested models in the table. To protect our data from malicious users we can implement encryption. This also describes various forms of encryption. Using encryption, we can safe our confidential information. Then we discuss different types of security related to cloud in our paper and provide their solutions. Security must be different types like information, software etc. In addition, we draw architecture of cloud computing which include different services like IaaS, PaaS and IaaS each have different functionalities and responsibilities and define these with their examples properly. This study shows that CC provide facility to use the resources from resource pool that help in reducing the E-Waste. Some benefits of cloud based computing are indicating in our paper that be able to very helpful. Around here are numerous problems in CC require to be studying in the next research like that assurance, privacy, achievement, possession and other non-technical concerns. Thus, scholars are confronting much problems and requires to identify results for the engineering and non-technical problems.

10. Conclusion and Future Work

Cloud computing has such versatility, efficiency, usability and cost savings characteristics, which are very motivating. It is the latest emerging technology, which offers users many benefits; it faces many securities. Data security issues and approaches to such issues are presented here to address the threats involved in CC. In this paper we have eloborated certain uses of cloud computing. This study show that implementing this technology in an organization after teckling the data related security issues can bring a diractic change. Here we have discussed some important data security issues in cloud computing, solution of that problems, prons and cons of cloud computing. This study shows that CC provide facility to use the resources from resource pool that help in reducing the E-Waste. In future study, there are many concerns in cloud that need to be evaluated such as protection, privacy, efficiency, property, profitability and other non-technical issues. Research teams therefore face many obstacles and require studying the solutions for the technological and non-technical problems. The security problems required to be intensively examined.

References

[1] Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. "Security and privacy challenges in cloud computing environments." *IEEE Security & Privacy* 8.6 (2010): 24-31.

[2] Bassi, Sonia, and Anjali Chaudhary. "Cloud Computing Data Security–Background and Benefits." *International Journal of Computer Science & Communication* 6.1 (2015).

[3] On technical security issues in cloud computing, Meiko Jensen etal, 2009

[4] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud definition, in:ACM SIGCOMM Computer Communication Review, 2008.p.50-55

[5] M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6.

[6] Ensuring Data Storage security in cloud computing, Cong Wang, etal, 2010

[7] Privacy reserving, Cong Wang etal, 2010

[8] Data Security in the world of cloud computing, John Harauz, etal, 2010

[9] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34(1), Jan.2011, pp. 1–11.

[10] B. Gupta, D. P, "Handbook of research on modern cryptographic solutions for computer and cyber security," IGI Global, 2016.

[11] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[12] Bairagi, Swati I., and Ankur O. Bang. "Cloud Computing: History, Architecture, Security Issues." *National Conference "CONVERGENCE*. Vol. 2015. 2015.

[13] Kaufman, Lori M. "Data security in the world of cloud computing." *IEEE Security & Privacy* 7.4 (2009): 61-64.

[14] A brief history of cloud computing By Keith D. Foote on June 22, 2017

[15] Hussein, Nidal Hassan, and Ahmed Khalid. "6." *International Journal of Computer Science and Information Security* 14.1 (2016): 52.

[16] Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges"

[17] F. Maggi and S. Zanero. Rethinking security in a cloudy world. Techni-cal report, Technical report, Dipartimento di Elettronica e Informazione,Politecnico di Milano, 2010.

[18] Md Tanzim Khorshed, A. B. M. Ali, and Saleh A. Wasimi. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems, 2012

[19] F.B. Shaikh and S. Haider. Security threats in cloud computing. In Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, pages 214 –219, December 2011.

[20] Eystein Mathisen. Security challenges and solutions in cloud computing. In Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on, pages 208–212, 2011.

[21] L. Ertaul, S. Singhal, and G. Saldamli. Security challenges in cloud com-puting.California State University, East Bay. Academic paper http://www.mcs. csueastbay. edu/ lertaul/Cloudpdf, 2009.

[22] Wentao Liu. Research on Cloud Computing Security Problem and Strategy, in:2nd International Conference on Consumer Electronics. Communications and Networks (CECNet), April 2012.p.1216-1219.

[23] Eman M.Mohamed, Hatem S Abdelkader, Sherif EI Etriby. Enhanced Data SecurityModel for Cloud Computing, in:8th International Conference on Informatics and Systems(INFOS), Cairo,May 2012.p.12-17.

[24] Rao, R. Velumadhava, and K. Selvamani. "Data security challenges and its solutions in cloud computing." *Procedia Computer Science* 48 (2015): 204-209.

[25] Aldossary, Sultan, and William Allen. "Data security, privacy, availability and integrity in cloud computing: issues and current solutions." *International Journal of Advanced Computer Science and Applications* 7.4 (2016): 485-498.

[26] Karajeh, Huda, Mahmoud Maqableh, and R. Masa'deh. "Privacy and Security Issues of Cloud Computing Environment." *Proceedings of the 23rd IBIMA Conference Vision 2020*. 2016.

[27] Aldossary, Sultan, and William Allen. "Data security, privacy, availability and integrity in cloud computing: issues and current solutions." *International Journal of Advanced Computer Science and Applications* 7.4 (2016): 485-498.

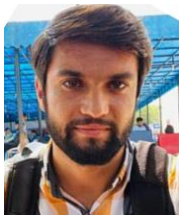
[28] Bairagi, Swati I., and Ankur O. Bang. "Cloud Computing: History, Architecture, Security Issues." *National Conference "CONVERGENCE*. Vol. 2015. 2015.

[29] D. Daniels, "Identity Management Practices and Concerns in Enterprise Cloud Infrastructures," J-Gate Acad. J. Database, vol.II, no. 14, 2013, pp. 2321–5518.
[30] S. Hajra et al., "DRECON: DPA Resistant Encryption by Construction," Springer, 2014, pp. 420–439.
[31] A. Tripathi and A. Mishra, "Cloud computing security considerations," IEEE Intl.Conference on 90Signal Processing, Communications and Computing (ICSPCC), 2011, pp. 1–5
[32] "SANS Institute: Network Security Resources." [Online]. Available: 91https://www.sans.org/network-security/. [Accessed: 16 Feb. 2017]
[33] M. Al Morsy, J. Grundy, and I. Müller, "An Analysis of the Cloud Computing Security Problem,"APSEC Cloud W., Nov.2010.
[34] K. M. Khan and Q. Malluhi, "Establishing Trust in Cloud Computing," IT Prof., vol. 12 (5), Sept. 2010, pp. 20–27.
[35] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," Theor. Comput. Sci., vol. 422, Mar.2012, pp. 15–38.
[36] S. Ramgovind, Mariki M. Eloff, and E. Smith. The management of securityin cloud computing. InInformation Security for South Africa (ISSA), 2010, pages 1–7, 2010.

Authors' Profiles

Sadia Anayat is doing her BS (Hons) in Computer Science (CS) from Govt College Women University Sialkot. She is also certified as Microsoft Office specialist. Thwo of her paper has been published recently. Now she is working on research in Blochain technology and comparison between bitcoin and ethereum, cloud computing and green computing topic. Her main areas of research interest are blockchian technology.

Isma Zulifqar is doing her BS (Hons) in Computer Science (CS) from Govt College Women University Sialkot. One of her paper is published recently. Currently she has been working on research as final year project in Data Diversity in Medical IoT topic. Her main areas of research interest are Cloud Computing, primary dangerous computer viruses, DataBa



Imtiaz Kharal is currently doing his BS in computer science from Islamia University of Bhalwapur, Pakistan.

How to cite this paper: Isma Zulifqar, Sadia Anayat, Imtiaz Khara, " A Review of Data Security Challenges and their Solutions in Cloud Computing", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.13, No.3, pp. 30-38, 2021. DOI: 10.5815/ijieeb.2021.03.04