Backup & Data Recovery in Cloud Computing: A Systematic Mapping Study

Msc. Roland PLAKA

Abstract

Context: Digital data is being stored in large quan- tities in Cloud, requiring data backup and recovery services. Due to many factors such as disasters and other disruptive events, the risk of data loss is huge. Therefore, backup and data recovery are essential and effective in improvement of system availability and maintaining Business Continuity. Nevertheless, the process to achieve the goal of business uninterrupted faces many challenges regarding data security, integrity and failure prediction. Objective: This paper has the following goals: analyzing system- atically the current published research and presenting the most common factors leading to the need of Disaster Recovery and backup plan; investigating and identifying the adopted solutions and techniques to prevent data loss; and lastly, investigating the influence Data Recovery and Backup has in terms of business continuity and identifying the privacy and security issues regard- ing disaster recovery process. Method: A systematic mapping study was conducted, in which 45 papers, dated from 2010 to 2020 were evaluated. Results: A set of 45 papers is selected from an initial search of 250 papers, including 10 papers from snowball sampling, following the references from some paper of interest. These results are categorized based on the relevant research questions, such as causes of disasters, data loss, business continuity, and security and privacy issues. Conclusion: An overview of the topic is presented by investigating and identifying the following features: challenges, issues, solutions, techniques, factors, and effects regarding the backup and recovery process.

***Keywords**: Cloud Computing, Backup, Data Recovery, Disas- ter Recovery, Data loss, Business Continuity, Data Security, Data Privacy.*

I. Introduction

In today's globalized world, the notion of Cloud Computing is becoming a remarkably familiar approach in terms of scope and services to be provided. As we know, most of the data and applications are found and stored digitally, all over the world, on-premise hardware, or off-premise computing. This means, that the possibilities of data storage in the cloud can be endless, but so are also the data. The amount of data is heavily increasing day by day, and the necessity to store these data in the cloud comes in a straight proportion to it. Therefore, Cloud Computing services varies in different types based on demand and requirements.

In this paper, our focus will be to investigate Backup and Data Recovery, as they play an essential and significant role when it comes to Cloud Computing and the offered services. Since most of the data are sensitive and incredibly important in various domains, the need for a Backup and Recovery plan is vital. And no matter in what perspective or level we start to analyze, (e.g. personal data, sensitive data public data, confidential data, etc.) whether they are translated as qualitative or quantitative, at some point, the need for the backup will be crucial. Especially when it comes to big companies and organizations where data is "life-and-death" to their existence.

The risk of data loss is relatively high regardless of the cloud environment, provider, services, or architecture. No matter if the data are stored in a Public or Private Cloud, data can still be corrupted at any stage. Therefore, to maintain the data safety, control, and accessibility it is required a strategy, including a backup and disaster recovery plan.

A disaster recovery plan can be the best solution for a disaster event, whether it is man-made or natural type. Since these disasters can lead to hazards and devastating damage to a system, as a result, data availability and accessibility can be compromised. We have identified 4 types of disasters based on their nature: Climate Disaster; Intended Disruption; Loss of Utilities and Services; Equipment or system failure. Besides, if one of these disasters happens and data gets corrupted or damaged, it can lead to a full data loss.

Therefore, the need for some mechanisms and methods of backup and data recovery is a priority for many customers who have trusted the data on the cloud. And the purpose of these recovery techniques is to ensure the customers and businesses to collect the information from any backup server, when server fails to provide the data to the user.

In recent years, there has been an increased interest in Backup and Data Recovery, however, when we get to look at the literature there is relatively a low amount

of research and papers regarding the topic. Hence, in this paper, we will focus on highlighting and discussing the found research, done on backup and disaster recovery in cloud computing. The main issue that we have encountered related to disaster recovery in cloud computing is the concern to provide an effective plan that ensures high data reliability and security. Nevertheless, an overview of the most important key factors regarding the topic, will be discussed and be found in this paper.

For a wide overview of the Backup and Data Recovery in Cloud Computing research area, we have used the systematic mapping study approach [1] to collect data, analyze and interpret results, regarding the scope of interest and the evidence collected in the papers.

This paper is organized as follows: in Section II is shown related work; Section III presents background and motivation for the study; In Section IV we describe the systematic mapping study approach from the selection of the papers to classifying and lastly analyzing the results for each research question; in Section V we show the results we gathered for answering research questions; and finally, Section VI draws conclusions and outlines related to our systematic mapping study.

II. Related work

Our work attempts to conduct a systematic mapping study on backup and data recovery in cloud computing. In correspondence with [2] we identified the main factors and challenges of DR in cloud computing. It concludes that data DR services must ensure high data reliability and flexibility through an effective and practical DR plan that sustain growth for any organization. According to the authors, the most critical issues relevant to DR in cloud computing focus on cloud data storage, cost, security, lack of latency and redundancy. Different strategies attempt to manage the data recovery process. They also highlighted that natural and man-made disasters can result in costly service interruptions.

In the literature survey of [3] they found many techniques that have their unique ways to create backup and recovery. We illustrated these techniques in Tab 4. The experimental results, done by [4] shows that many organizations and companies have utilized disaster recovery solutions to minimize the downtime and data loss incurred when catastrophes take place. All these approaches aim to provide the best performance.

Organizations are subjected to hazards that might interrupt options. From the point of Service Provider, client satisfaction is among the major objective, while from the business aspect, recovery means being able to perform business functions without affecting continuity. DR services should assist business continuity, enabling

applications to quickly come back online after a disaster happens (Alshammari et al.,2016).

III. Background and motivation

In this section we emphasize the importance of data backup and recovery in cloud computing.

Data are valuable nowadays and if are lost, may cause a negative impact on the organization financial costs and time to regain it, so protecting important data, are required efficient countermeasures. During this decade cloud computing has become a new technological option to provide services and cloud providers are gaining even more popularity due to the increasing amount of data. The expanded usage of cloud computing services increments the need of more storage, backup and recovery.

Backup is defined as a duplication of any data, file, application and operating system that can be used in case of a data loss or restoration, while recovery is the set of techniques used to collect data from any backup server, when data are previously lost from the server or invalid to use.

Disasters effect both the client and the cloud side, hence it is crucial to have a disaster recovery plan. As it is mentioned by (A. Arul Mary, K. Chitra) when "disaster happens in customer side means backup will be stored in the cloud, but disaster happens in the cloud means data will be lost. So, disaster recovery process is urgently needed. But quality and security are the key issues in the information recovery process" [5].

Even though there are still many technological gaps, for many organizations, cloud computing is a flexible, cost- effectively, reliable and scalable solution to provide a safe data backup and recovery. The organizations must identify the major probable failures that can cause a disaster for them, then prepare a disaster recovery plan (DRP) and data backup.

DRP is a document that prepares and helps organizations to protect and prevent damages from a disaster. This plan usually addresses any type of disaster, however, it is customized based on the needs of the organization where the most important elements included are related to identifying and assessing disaster risks and determine the critical applications and resources.

This is crucial for their continuity, in order to protect themselves and employees from natural and man-made errors. Various techniques are proposed for this purpose, i.e. moving from single cloud to multi-cloud environment is considered as an empirical solution, however it has some legal issues to implement because of data security, privacy and authorization.

IV. Systematic mapping study

In this paper we present a systematic mapping approach adopted by [6]. Our study will be an overview in terms of solution, challenges, factors, security, and privacy, based in backup and data recovery literature. The methodology we embraced consists in four essential steps, however, Fig 1. describes best our process steps and outcomes.

- Identifying RQs.
- Searching for primary studies.
- Classification scheme of the relevant papers.
- Analyzing data and answering RQs.

FIG. 1. Systematic mapping process adopted by Peterson et al (2008).

A. Identifying research questions

The first step, and probably the most significant, is identifying and defining research questions [7]. As we mentioned earlier, our purpose is to have an overview of backup and data recovery, to understand its importance, to identify some challenges and solutions and how it affects different environments and domains in the context of cloud computing.

After we have discussed and evaluated some issues, we were able to formulate and define four research questions.

RQ1. What are the most common factors that can lead to the need of a Disaster Recovery and Backup plan?

- There are many factors that negatively influence a cloud environment and therefore they can lead to the necessity of a backup and data recovery. However, our focus is to present the most common factors that usually are identified, leading to such situation and needs.

RQ2. What are the methods and solutions used to prevent a full data loss?

- Various methods and solutions are presented nowadays to prevent data loss and avoid further damage for the data in the cloud. Our aim of the question is to investigate the most used solutions adopted for the backup and disaster recovery in order to identify some strategies that in many domains are needed.

RQ3. How will the Backup and Recovery process influence the business continuity?

- Since businesses are the most affected environments in a case of disaster and data loss in cloud, our objective is to investigate the influence these factors have in terms of business continuity.

RQ4. Which are the security and privacy measures in the data recovery?

- Our purpose of the last question is to investigate the finished process of data recovery in terms of security and privacy. How these aspects are covered and identifying the provided solutions are for this case.

TAB 1. The conducted search strings.

IEEE Xplore
("Backup" AND "Data Recovery") AND ("Cloud")

Scopus
(("Backup" AND "Data AND Recovery") AND ("Cloud"))

B. Searching for primary studies

The goal of this step is to create and conduct a search sting into the digital databases. The following digital databases were used in the search: IEEE Xplore and Scopus. After adopting many different strings we ended by evaluating the above mentioned. The same string that is used in IEEE database is used also for Scopus, however, a slightly automatic change has been made by the database. Since both strings work

perfectly on their respective database, and the results are suitable, the final result of the strings is conducted, and shown in Table 1.

a) Inclusion Criteria:

- The study must address an overview on Backup and Data Recovery in Cloud Computing.
- The study must have been published in the last 10 years, (i.e. 2010-2020).
- The study must have been published as a full document, in English (conference paper, journal paper, article).

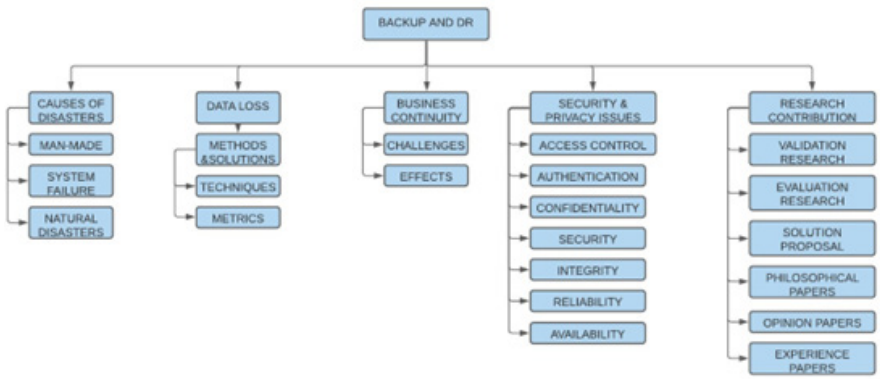
b) Exclusion Criteria:

- Papers which are outside the context of cloud computing.
- Papers which have not enough data/information to pro- vide an understanding of the case.
- Papers which evaluate the topic on a non-related perspec- tive.

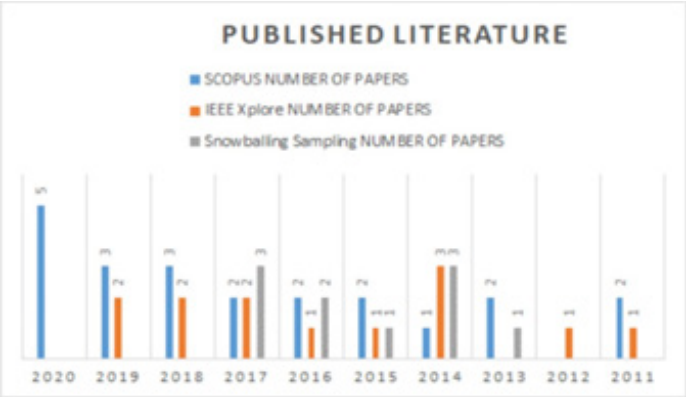
TAB 2. Databases and initial papers

Digital Database		Stage 1.	Stage 2.	Stage 3.
Scopus		156 papers	30 papers	16 papers
IEEE Xplore		94 papers	28 papers	19 papers
	Total	**250 papers**	**58 papers**	**35 papers**
Added 10 papers following the references from some paper of interest In total we had **45 papers**				

FIG 2. Classification Scheme



GRAPH 1. Published papers in 2011 - 2020 timeline



As it can be seen by the Graph 1. our selected papers are divided between 2011 to 2020 as per year 2010 there were no papers that interested us, related to the topic and content.

Most of the literature is published this year, 2020, and we must say that based on the classification by research type, our selected primary studies are published as a Solution Proposal with a total of 24 papers. In Tab 3. is shown the detailed classification based on the category and with their respective number of papers.

TAB 3. Primary studies classification by research type

Category	Paper Inxed	Nr. of Papers
Validation Research	e1,e7,p1,p14,p16,p28,p31,p34,p45	9
Evaluation Research	e3,e5,e6,e7,e9,p17,p21,p26,p27,p35	10
Solution Proposal	e2,e4,e9,e10,p2,p3,p4,p5,p8,p9,p10,p12,p13,p15 ,p24,p32,p34,p37,p38,p42,p44,p45,p46,p47	24
Philosophical Papers	e8,p18,p29,p30,p39,p41	6
Opinion Papers	p30,p39	2
Experience Papers	p29	1

C. Screening

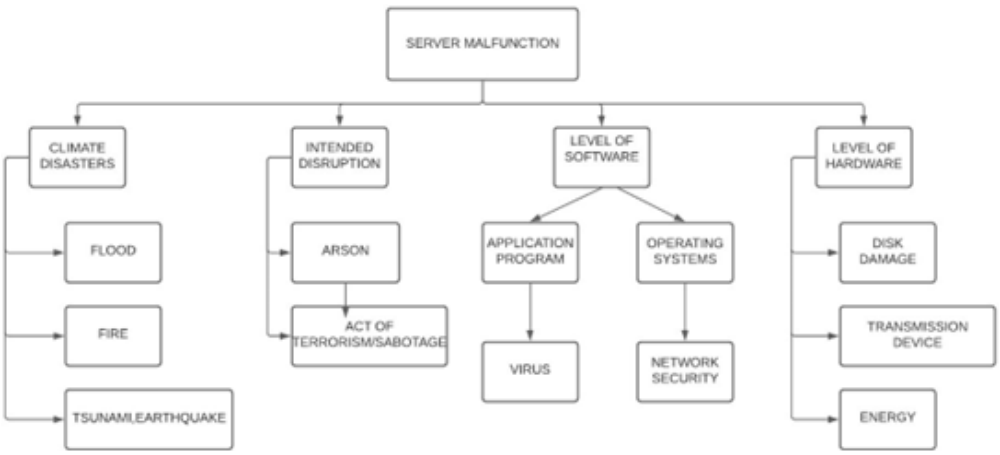
- Stage 1: The definition of search string in both databases gave us in total 250 papers.
- Stage 2: Applying inclusion and exclusion criteria in title, abstract and keywords we reduced the number of papers into 58 papers. Duplicated papers were avoided also.
- Stage 3: Next, we selected the remaining papers based on conclusion and often other sections as we found important to our study. In total we have 35 papers to read as a full text.

Lastly, we found and added 10 papers to our list, following the references from some paper of interest. At the end, each paper has been indexed with a ”random name” as a matter of ease. i.e., p1, p2... for primary studies papers (selected by the two databases) and e1, e2... for the snowball sampling (selected by following the references of the previous papers).

D. Classification scheme for the relevant papers

In order to create the classification scheme (shown in Fig 2.) we have categorized different ”sections/topics”, based on their similarities. However, a category is created as a result of the key focus related to our RQs. The top level, which is the root, is our main topic. And the other categories are influenced by our analysis and the need to answer our research questions. The first thing we applied was keywording. It was applied to titles, keywords and abstracts, however, most of the time some of these sections had poor quality leading us moving to the next sections of the papers. So this process was done in the full text of every relevant paper. After we finished this process we started to evaluate and define the contribution for paper regarding our study. About the research contributions, we have previously shown in tab 3. For RQ1, which shows the causes of disasters, three categories were identified: Man-made disasters, Natural disasters, and System failure. Then, for RQ2, related to data loss we have identified some methods and solutions and two sub-categories were created: techniques and metrics. Next, for RQ3 regarding business continuity we have identified and discussed about challenges, solutions, techniques and the effects they have in BC. Lastly, for RQ4 we have listed some security and privacy issues based on the risks.

FIG 3. Factors that lead to a Disaster Recovery and Backup plan



V. Results

The selected papers for this study are 45 papers. From which 35 papers have been selected as a result of our screening procedure and applying inclusion and exclusion criteria, and 10 papers are added following the reference of our papers of interest. The distribution by year is shown in Graph 1.

A. Results of RQ1

RQ1: What are the most common factors that can lead to the need of a Disaster Recovery and Backup plan?

Disaster Recovery plans are a set of procedures and policies used to restore the high priority processes of a system after a disaster. In addition, DRP is vital to define and ensure all the responsibilities that everyone should follow when a disaster happens, to enable the restoration of these processes and data. This process helps to minimize impact and damages and recover data when a loss occurs, by responding on time. A well-trained staff, necessary resources and assets makes the perfect combination to withstand and prevent a catastrophic failure of the system.

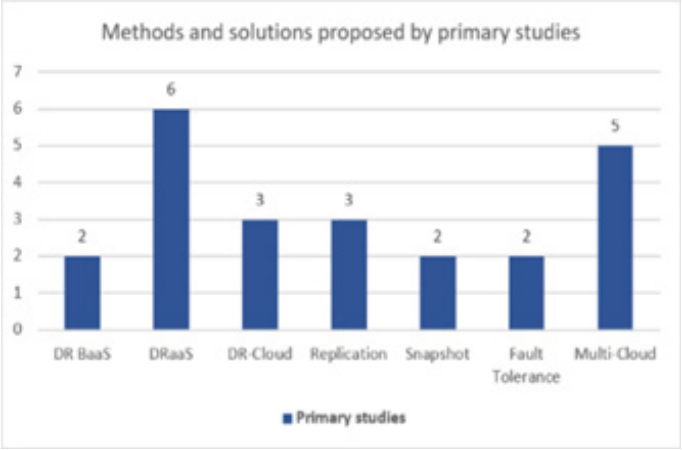
Above all, organizations should apply routine controls to prevent these factors before they occur unexpectedly. Disaster Recovery and backup still are not on effortless way of backing up cloud data into devices, due to lack of control over cloud assets. Generally, customers store sensitive data on single clouds, but recovery and data backup consume huge storage by replicating data to multiple data centers. For this reason, depending on single clouds contains the above-mentioned risks. These factors are shown in Fig 3. and can lead to disruption of the services, data loss even can cause a collapse of the entire system [8]. Fig 3. has been created as a result of analysing the following papers: [p1], [p3], [p4], [p9], [p13], [p21], [p29], [p35], [p41].

B. Results of RQ2

RQ2: What are the methods and solutions used to prevent a full data loss?

During our study we have noticed many solutions that have been discussed and proposed as a method or a strategy that will ensure zero data loss and a quick recovery process [9]. However, we came in the conclusion that none of these methods/solutions will be 100% efficient in every aspect, especially when it comes to reliability and security of data after a recovery process.

GRAPH 2. Adopted solutions and methods to prevent data loss



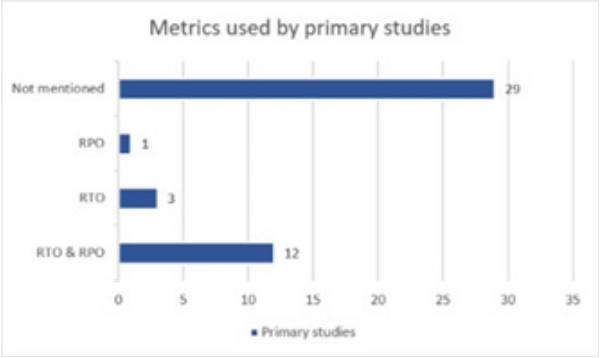
TAB 4. Existing techniques to backup data

Recovery mechanisms	*Studies*						
	e3	**e5**	**e6**	**e8**	**p16**	**p30**	**p39**
RAID		x					x
HAIL		x		x			
HSDRT			x		x	x	x
ERGOT			x		x	x	x
LINUX BOX			x		x	x	x
PCS			x		x	x	
RACS		x		x			
Cold and Hot backup	x				x	x	x
DeepSky		x		x			

An important recommendation to prevent data loss and meet a variety of needs such as availability, business continuity and disaster recovery is to engage in a Multi-Cloud strategy. But, if we must mention some used strategies in our analysis, we can also highlight replication and snapshot in different environments. However, as we can see from Graph 2, the most discussed solution in terms of disaster recovery as a way to prevent data loss is the introduction and adoption of a service model known as Disaster-Recovery-as-a-Service (DRaaS) [10]. The rest of the solutions are shown in the graph 3.

When it comes to techniques, the most common one is plain backup. As it is one of our focuses, we must say that some papers have described it as a not convenient technique due to security and reliability problems. And in order to overcome these problems, there are addressed data backup and recovery mechanisms and techniques in a more safe and effective system [11]. These techniques are shown in tab 4.

GRAPH 3. RTO & RPO metrics used in the studies



Disaster Recovery and Backup plan consists of some pa- rameters, but the fundamentals are defined as metrics, and the most common are RTO and RPO. These metrics are used to measure the recovery level which should be a focus when describing a disaster recovery plan in terms of tiers.

- RTO – Recovery time object; The time of the physical system recovery after a disaster happened.
- RPO – Recovery point object; The latest backup before the disaster. Meaning the quantity of data loss [12].

C. Results of RQ3

RQ3: How will the Backup and Recovery process influence the business continuity?

Business Continuity (BC) is a methodology and concept to manage elements that allow a business to function normally during and after a disaster [8]. In order to have maintain business continuity it is necessary to have a clear plan and strategy regarding a disaster event and data recovery. The plan must allow the organization to achieve the following services [8].

- Immediate & Proper response to disruptive events
- Reduce business impact
- Ensure business continuity services
- Reduce business impact

As we already can understand that BC is a very important requirement for any organization whose data are stored in cloud, we also must mention that it has its challenges. And often these challenges can be fatal for a business if a proper solution and technique is not immediately found and adopt.

After reviewing 13 papers related and discussing about Business Continuity in terms of Cloud Computing, we found the following challenges in Disaster Recovery that can influ- ence negatively in BC. These challenges are shown in tab 5.

TAB 5. Challenges in Disaster Recovery that influence BC

Challenges	Papers								
	e2	e4	e9	p1	p19	p21	p29	p39	p41
Dependency		x			x	x	x		x
Cost		x			x	x	x		x
Failure Detection	x	x		x	x	x	x	x	x
Security Detection	x			x	x	x	x		x
Replication Latency	x				x	x	x		x
Data Storage	x		x		x	x	x		x
Lack of Redundancy		x	x		x	x	x		x

However, along with the challenges, every paper hasmentioned at least one solution and techniques that could improve the disaster recovery plan and maintain a flexible and effective business continuity.

Solutions presented in papers:

- Block Replication.
- Cloud-Based DR.
- Local Backup.
- Multi-Cloud strategy.
- Replication of backup in multiple data centers.
- Pipelined Replication.
- Hot Standby (Active/Active).

All these solutions and many more are discussed in [e2] [p10] [p12] [e9] [e4], helping in terms of business continuity in different aspects. I.e., Block Replication will ensure to achieve zero RTO and negligible RTO [8] [9]; Local Backup will have minimal cost and ensure peace of mind [12]; Multi-Cloud environment will minimize the risk of availability failure, loss of data and privacy [13]; Hot Standby (Active/Active) is a synchronous real-time replication in based in database backup and ensures both RTO RPO to be zero, meaning 0 data loss [14].

In terms of adopted techniques, we can say the most common and mentioned one is Linux Box. However, techniques can be different based on the issue and challenge [15], [16], [17], [18], [19], [20], [21], I.e., if the challenge is Data storage and lack of redundancy, a suggested technique by [p29] is using an inter private cloud and multiple backups. Using monitoring units, encryption, scrambling and shuffling techniques can also be a solution for failure and security challenges.

In overall, as a conclusion for every paper related to BC, backup and disaster recovery in mentioned as a vital requirement to ensure the organization functionality

even during or after a disaster or disruptive event. It might be heavy in terms of costs; however, it guaranties the ability to work uninterruptedly regardless the nature of the disruption. A business continuity plan provides guidance to IT staff to follow the emergency plan, to recover and resume the business functionality and operations [8].

If business continuity is not ensured, the organization will have massive negative effects, such as, losses of receipts, business reputation, market share, etc. And often, it can lead to the worst-case scenario which is the collapse of the entire organization.

At this stage we can all evaluate the importance of the Backup plan and data recovery, and how it influences the business continuity. On the end, businesses are forced to make the decisions between cost, speed and effectiveness of recovery.

D. Results of RQ4

RQ4: Which are the security and privacy measures in the data recovery?

TAB 5. Security and privacy issues to data recovery

Access Control	p5, p13, p14, p28, p24
Authentication	p5, p13, p14, p15, p30, p31, p32, p39
Confidentiality	p2, p5, p12, p13, p14, p19, p21, p41
Security	p1, p29, p41, p3, p5, p13, p14, p15, p16, p12, p21, p30, p26
Integrity	p15, p32, p5, p12, p13, p14, p15
Reliability	p15, p17, p5, p2, p4, p12
Availability	p16, p12, p13, p19, p21

Data recovery is mentioned as one of the most critical security issue in cloud computing. DR process should be distributed over multiple sites for full data recovery. Recovery techniques and mechanisms help to collect information from the backup server when a crash happens. To provide cloud services there is a need to satisfy the clients about the reliability of their data. Ensuring a full DR is not an easy task for SP. The main concern is solving the problems of data access and authorization for multiple users. In this paper, we will present the most common security issues.

- Access control means full protection of data.
- Integrity is the process of verifying the data stored in the cloud.
- Confidentiality is related to fault-tolerance and access controls protocols.

When users join the network, authentication on the cloud server must be unique. Successful authentication means access to web services. Security matters occur due to insufficient certification, authorization, audit control, week encryption

algorithms, and unstable data centers (Alshammari et al.,2016). Privacy concerns are related to reliability and authorization controls to protect users.

Users hesitate to upload their critical data to the cloud servers because they don't believe that cloud service providers can guarantee privacy protection (Song et al.,2011).

Privacy protection is a crucial issue for providing personal data recovery services. On the other hand, encryption based data protection is proposed as a solution to solve this problem. It is important that data transfer between user and machine be secure. The privacy should be preserved by not leaking the data during the integrity verification process [11].

VI. Conclusion

In this paper we introduce a Systematic Mapping Study on Backup and Data Recovery in Cloud Computing. The timeline of the study is from 2010 to 2020, and we were able to extract the data from a total of 45 papers. In where 35 papers have been selected as a result of screening process by applying inclusion and exclusion criteria, and the other 10 papers were added following the references from some paper of interest. The initial number of papers was 250, obtained from IEEE Xplore and Scopus.

Regarding the RQs, there are 9 papers that discuss about causes of disasters as the main factor that lead to the need of DR and Backup plan. Then, related to the solutions and techniques proposed by 16 papers, we were able to list some of them where the most discussed one was Disaster Recovery-as-a-Service as a model and service to adopt, and followed by Multi-Cloud strategy which guaranties quick recovery and business continuity.

In addition to BC, we followed and identified a chain of factors such as challenges, solutions, and techniques influencing in the overall backup an DR plan process.

Lastly, regarding the most important issues in data recovery we can mention Security (discussed in 13 papers), Authenti- cation & Confidentiality (discussed in 8 papers), and followed by Integrity (discussed in 7 papers). However, some other important issues consist of Reliability, Availability and to the Access of Control.

All these aspects are treated as issues and gaps, in which is required more improvement in order to have a complete and successful data recovery.

References

[1]K. Peterson, S. Vakkalanka, L. Kuzniarz, ”Guidelines for conducting systematic mapping studies in software engineering: An update” Infor- mation and Software Technology 64 (2015) pp. 1-18.

[2]A. Abualkishik, A. Alwan, Y. Gulzar, ”Disaster Recovery in Cloud Computing Systems: An Overview”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 9, 2020.

[3]K. Sharma, K. R Singh, ”Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 5, November 2012.

[4]R. Matos, E. Andrade, P. Maciel, ”Evaluation of a Disaster Recovery Solution through Fault Injection Experiments”, 2014 IEEE International Conference on Systems, Man, and Cybernetics October 5-8, 2014, San Diego, CA, USA.

[5]A. Arul Mary, K. Chitra, ”OGSO-DR: oppositional group search op- timizer based efficient disaster recovery in a cloud environment” J Ambient Intell Human Comput 10, 1885–1895 (2019).

[6]K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson, ”Systematic Mapping Studies in Software Engineering” June 2008.

[7]J. Mendonc¸a, E. Andrade, P. Endo, R. Lima, ”Disaster recovery solutions for IT systems: A Systematic mapping study” Journal of Systems and Software, Volume 149, March 2019, Pages 511-530.

[8]M. M. Al–shammari and A. A. Alwan, ”Disaster Recovery and Business Continuity for Database Services in Multi-Cloud,” 2018 1st International Conference on Computer Applications Information Security (ICCAIS), Riyadh, 2018, pp. 1-8.

[9]Z. Saquib, V. Tyagi, S. Bokare, S. Dongawe, M. Dwivedi and J. Dwivedi, ”A new approach to disaster recovery as a service over cloud for database system,” 2013 15th International Conference on Advanced Computing Technologies (ICACT), Rajampet, 2013, pp. 1-6.

[10]R. Matos, E. C. Andrade and P. Maciel, ”Evaluation of a disaster recovery solution through fault injection experiments,” 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC), San Diego, CA, 2014, pp. 2675-2680.

[11]S. Suguna and A. Suhasini, ”Overview of data backup and disaster recovery in cloud,” International Conference on Information Communi- cation and Embedded Systems (ICICES2014), Chennai, 2014, pp. 1-7.

[12]V. Javaraiah, ”Backup for cloud and disaster recovery for consumers and SMBs,” 2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), Bangalore, 2011, pp. 1-3.

[13]M. M. Alshammari, A. A. Alwan, A. Nordin and I. F. Al-Shaikhli, ”Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges,” 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), Salmabad, 2017, pp. 1-7.

[14]T. Zhu, Y. Xie, Y. Song, W. Zhang, K. Zhang, F. Gao, ”IT Disaster Tolerance and Application Classification for Data Centers”, International Congress of Information and Communication Technology (ICICT 2017), Volume 107, 2017, Pages 341-346.

[15]H. Wang, "A Warm-CDP Backup System", International Congress of Information and Communication Technology (ICICT 2017) pp. 80 - 83.
[16]S. Wu, K.-Ching Li, B, Mao, M. Liao, "DAC: Improving storage availability with Deduplication-Assisted Cloud-of-Clouds", Future Gen- eration Computer Systems, Volume 74, September 2017, Pages 190-198.
[17]S. Suguna, A. Suhasini, "Enriched multi objective optimization model based cloud disaster recovery", Karbala International Journal of Modern Science, Volume 1, Issue 2, October 2015, Pages 122-128.
[18]M. Tebaa, S. EL Hajji, "From Single to Multi-clouds Computing Privacy and Fault Tolerance", 2014 International Conference on Future Information Engineering, Volume 10, 2014, Pages 112-118.
[19]G. H. Pandurang, C. S. Bhimrao and P. Chothe, "Data recovery through indexing in cloud computing," 2016 International Conference on Com- munication and Electronics Systems (ICCES), Coimbatore, 2016, pp. 1-5.
[20]K.R. Singh, "Online Data Backup and Disaster Recovery Techniques in cloud computing: A Review" International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 5, November 2012.
[21]S. Suguna and A. Suhasini, "Overview of data backup and disaster recovery in cloud," International Conference on Information Communi- cation and Embedded Systems (ICICES2014), Chennai, 2014, pp. 1-7.

Appendix
ID Reference

p1 Victor Chang," Towards a Big Data system disaster recovery in a Private Cloud", Ad Hoc Networks, Leeds, vol nr. 35, 2015, pp. 65-82
p2 Bardis N.G., Doukas N., Markovskyi O.P.," A Method for Cloud Storage Data Recovery with Limited Loss of Access", Proceedings - 2017 4th International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2017, vol nr.2018-January,2018, pp.128-133
p3 Faria H., Solís P., Bordim J., Hagstrom R.," A backup-as-a-service (BaaS) software solution", CLOSER 2019 - Proceedings of the 9th International Conference on Cloud Computing and Services Science, Brasilia,2019, pp.225-232
p4 Zhong R., Xiang F.," A cost aware backup strategy in hybrid clouds", Proceedings - 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content, IC-NIDC 2012, Beijing, 2012, pp.256-260
p5 Tyagi M., Manoria M., Mishra B.," A Framework with Ciphertext Attribute-Based encryption for data security in the cloud", Proceedings - 2019 International Conference on Electrical, Electronics and Computer Engineering, UPCON 2019,2019, India
p8 Su Z., Xu Q., Luo J., Pu H., Peng Y., Lu R.," A Secure Content Caching Scheme for Disaster Backup in Fog Computing Enabled Mobile Social Networks", IEEE Transactions on Industrial Informatics, vol nr. 14, 2018 pp.4579-4589
p9 Arul Mary A., Chitra K.," OGSO-DR: oppositional group search optimizer based efficient disaster recovery in a cloud environment", Journal of Ambient Intelligence and Humanized Computing, Springer-Verlag GmbH Germany, vol.nr 10, pp.1885-1895

p10 Javaraiah V.," Backup for cloud and disaster recovery for consumers and SMBs", International Symposium on Advanced Networks and Telecommunication Systems, ANTS, Bangalore,2011
p12 Al-Shammari M.M., Alwan A.A.," Disaster Recovery and Business Continuity for Database Services in Multi-Cloud", 1st International Conference on Computer Applications and Information Security, ICCAIS 2018, Kuala Lumpur, 2018
p13 Kulkarni N.N., Jain S.A.," Checking integrity of data and recovery in the cloud environment", Indonesian Journal of Electrical Engineering and Computer Science, Maharashtra, 2019, vol nr.13, pp. 626-633
p14 Chen Z., Yao W., Wang C.," Security and Trust Model for Data Disaster-Recovery Service on the Cloud", Communications in Computer and Information Science, Beijing, 2013, vol nr.210, pp.140- 147
p15 Gokulakrishnan S., Gnanasekar J.M.," Data Integrity and Recovery Management in Cloud Systems", Proceedings of the 4th International Conference on Inventive Systems and Control, ICISC 2020, Chennai, pp.645-648
p16 Pandurang G.H., Bhimrao C.S., Chothe P.," Data recovery through indexing in cloud computing", Proceedings of the International Conference on Communication and Electronics Systems, ICCES 2016, Sangola.
p17 Alshammari M.M., Alwan A.A., Nordin A., Abualkishik A.Z.," Data backup and recovery with a minimum replica plan in a multi-cloud environment", International Journal of Grid and High- Performance Computing, International Islamic University Malaysia, 2020, vol nr.12, pp.102-120
p19 Alshammari M.M., Alwan A.A., Nordin A., Al-Shaikhli I.F.," Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges", 4th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2017, Kuala Lumpur, 2018, vol nr. 2018- Januart, pp. 1-7
p21 Tamimi A.A., Dawood R., Sadaqa L.," Disaster recovery techniques in cloud computing", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT 2019 – Proceedings, Amman, 2019, pp.845-850
p24 Gu Y., Wang D., Liu C.," DR-Cloud: Multi-Cloud based disaster recovery service", Tsinghua Science and Technology, Beijing, vol nr. 19, pp. 13-23
p26 Mendonça J., Lima R., Andrade E.," Evaluating and modelling solutions for disaster recovery", International Journal of Grid and Utility Computing, Recife, vol nr.11, pp.705-713
p27 Mendonca J., Lima R., Queiroz E., Andrade E., Kim D.S.," Evaluation of a Backup-as-a-Service Environment for Disaster Recovery", Proceedings - International Symposium on Computers and Communications, vol 2019-June
p28 Beineke K., Nothaas S., Schoettner M.," Fast parallel recovery of many small in-memory objects", Proceedings of the International Conference on Parallel and Distributed Systems – ICPADS, vol 2017-December, pp.248-257
p29 Mohammad M. Alshammari, Ali A. Alwan, Imad Fakhri Al-Shaikhli, "Data recovery and business continuity in Cloud computing: A Review of the Research Literature", International Journal of Advancements in Computing Technology · December 2016,Kuala Lumpur, vol nr.8, 2017
p30 Kruti Sharma, Kavita R Singh," Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review", International Journal of Engineering and Innovative Technology (IJEIT), Nagpur, vol nr.2, 2012

p31 Chavhan S., Patil P., Patle G.," Implementation of improved inline deduplication scheme for distributed cloud storage", Proceedings of the 5th International Conference on Communication and Electronics Systems, ICCES 2020, Nagpur,pp.1406-1410
p32 Poonam M. Pardeshi, Prof. Bharat Tidke," Improving Data Integrity for Data Storage Security in Cloud Computing", International Journal of Computer Science and Information Technologies, Vol. 5, Maharashtra, 2014, pp.6680-6685
p34 Harwalkar S., Sitaram D., Jadon S.," Multi-cloud DRaaS using OpenStack Keystone Federation", Proceedings of the 2019 International Conference on Advances in Computing and Communication Engineering, ICACCE 2019, Bangalore
p35 Silva B., Matos R., Tavares E., Maciel P., Zimmermann A.," Sensitivity analysis of an availability model for disaster tolerant cloud computing system", International Journal of Network Management, Recife ,vol nr.28, 2018
p37 Yuan R.-C., Lin J.-H., Li L.-X., Li Q., Di F.-C., Zhu Y.-K., Li Z.-J.," The optimize design of power integrated dispatching distributed inter-backup system", Asia-Pacific Power and Energy Engineering Conference, Beijing,APPEEC,2012
p38 Cherkasova L., Zhang A.," Optimizing QoS, performance, and power efficiency of backup services", 2015 Sustainable Internet and ICT for Sustainability, SustainIT 2015, CA 94304
p39 Suguna S., Suhasini A.," Overview of data backup and disaster recovery in cloud", International Conference on Information Communication and Embedded Systems, ICICES 2014, Chennai,
p41 Abualkishik A.Z., Alwan A.A., Gulzar Y.," Disaster recovery in cloud computing systems: An overview", International Journal of Advanced Computer Science and Applications, 2020, vol nr.11, pp.702-710
p42 Song C.-W., Park S., Kim D.-W., Kang S.," Parity cloud service: privacy-protected personal data recovery service", c. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011,2011, Seoul
p44 Prabhjeet Kaur, Gaurav Somani," Secure VM Backup and Vulnerability Removal in Infrastructure Clouds", Ajmer
p45 Hua Y.," Smart hashing based queries in the cloud", 2015 IEEE 23rd International Symposium on Quality of Service, IWQoS 2015,2016, Wuhan
p46 Lin L., Pan L., Liu S.," Backup or Not: An Online Cost Optimal Algorithm for Data Analysis Jobs Using Spot Instances", IEEE Access,Jinan,2020, pp.144945-144956
p47 Taguchi Y., Yoshinaga T.," System Resource Management to Control the Risk of Data-Loss in a Cloud-Based Disaster Recovery", Proceedings - International Computer Software and Applications Conference,2018, vol nr.2
e1 Xigao Li1·Lin Qian," A hybrid disaster-tolerant model with DDF technologyfor MooseFS open- source distributed file system", Springer Science+Business Media New York 2016,Nanjing
e2 Zia Saquib, Veena Tyagi, Shreya Bokare, Shivraj Dongawe, Monika Dwivedi, Jayati Dwivedi," A New Approach to Disaster Recovery as a Service over Cloud for Database system", Centre for Development of Advanced Computing, Mumbai,2013
e3 Hong wang," A Warm-CDP Backup System", International Congress of Information and Communication Technology (ICICT 2017), China
e4 Ermeson Andrade,Bruno Nogueira,Rubens Matos,Gustavo Callou,,Paulo Maciel," Availability modeling and analysis of a disaster-recovery-as-a-service solution", Springer-Verlag Wien 2017

e5 Suzhen Wu, Kuan-Ching Li, Bo Mao, Minghong Liao," DAC: Improving storage availability with Deduplication-Assisted Cloud-of-Clouds",vol nr.74, pp.190-198
e6 S. Suguna, A. Suhasini," Enriched multi objective optimization model based cloud disaster recovery", Karbala International Journal of Modern Science, 2015, Annamalai University, pp.122- 128
e7 Rubens Matos, Ermeson C. Andrade, Paulo Maciel," Evaluation of a Disaster Recovery Solution through Fault Injection Experiments", 2014 IEEE International Conference on Systems, Man, and Cybernetics, San Diego,2014
e8 Maha TEBAA, Said EL HAJJI," From Single to Multi-Clouds Computing Privacy and Fault Tolerance", 2014 International Conference on Future Information Engineering, Rabat,vol nr.10, pp.112-118
e9 Tielan Zhua, Yongqiang Xieb, Yang Songc, Weiguo Zhangb, Kai Zhangb, Fengyue Gaod," IT Disaster Tolerance and Application Classification for Data Centers", International Congress of Information and Communication Technology (ICICT 2017),Nanjing vol nr.107, pp.341-346
e10 Shubhashis Sengupta,K.M.Annervaz," Multi-site data distribution for disaster recovery—A planning framework", Future Generation Computer Systems, Nanjing, 2014, vol.nr 41, pp.53-64