Cloud services modeling for long-term intellectual capital protection

Saso Nikolovski[1], Bozidar Milenkovski[1], Anita Petreska[1]and Daniela Slavkovska[2]

[1] *Faculty of Information and Communication Technologies – Bitola, North Macedonia*
[2] *UTMS Skopje, Faculty of Computer Science, Republic of North Macedonia*

sasnik@gmail.com; bozidar.milenkovski@uklo.edu.mk; anita.petreska1@gmail.com; dslavkovska@yahoo.com

Abstract:
This paper presents a comprehensive performance evaluation framework to aid in the selection of optimal solutions for safeguarding and maintaining organizational data and information systems. The study emphasizes identifying critical factors and stages necessary for choosing a cloud-based solution tailored to business continuity and the protection of intellectual capital. The proposed framework facilitates selecting an adaptable recovery approach aligned with organizational operational needs, criticality of assets, and predefined timelines for business continuity and disaster recovery. Through detailed analysis and insights, this work supports informed decision-making in the implementation of reliable cloud services for resilience against outages or catastrophic events, ensuring sustained protection of an organization's intellectual capital.

Keywords:
Intellectual capital, disaster recovery, reliability, cloud service, business continuity, data protection, data recovery.

1. Introduction

In today's technology-driven business environment, companies increasingly depend on a robust Business Continuity Plan (BCP) to safeguard their intellectual capital. The development of these plans aims to ensure rapid recovery procedures following an outage or disaster. The unavailability of critical systems and services can have severe repercussions, including data loss and customer dissatisfaction, which ultimately impacts revenue and the value of an organization's intellectual assets.

From the aspect of the modern digitalized work environment, organizations aspire to achieve zero downtime during operational disruptions to ensure continuity and protect their intellectual capital. However, this ideal is often unattainable due to various potential disruptions, such as weather events or cyber attacks, despite the availability of numerous recovery solutions. These solutions range from on-premises data centers to cloud-based systems[1]. Consequently, organizational management increasingly prioritizes minimizing the impact of outages by assessing the maximum acceptable downtime that the business can sustain without compromising its intellectual assets or risking long-term operational consequences

Establishing an effective disaster recovery system that meets recovery plan requirements involves selecting solutions that align with specific utilization thresholds to uphold planned performance metrics. Prior research has often evaluated complex recovery solutions using a limited set of parameters, overlooking factors that directly influence the effectiveness of these implementations[2][3][4]. These include data transfer volume, system load during replication and recovery, and other conditions crucial for maintaining performance benchmarks.

Our research contrasts with prior studies by analyzing real-world data from an operational data center. We utilized these empirically validated parameters to develop a System Dynamics model, enabling us to assess how recovery solutions perform under various extreme conditions. This approach offers a deeper understanding of how to protect intellectual capital by ensuring reliable access to critical information assets in the face of potential disruptions.

2. Intellectual capital as the most important asset of the modern organizations

The development of knowledge, that is its embodiment in intellectual capital, today is a condition for economic, technological and any other form of progress in the knowledge based economy. The new way of creating values in the knowledge economy, through the management of intellectual capital and the continuous investment in it, points to the fact that for a modern organization is far more important the ability of employees to create value than the value of its tangible assets per se.

The intellectual capital of an organization represents its intangible assets as an important part of its total assets. This capital has a specific power creatively to turn the various types of knowledge, skills, structures, procedures, processes, technologies, etc. within an organization into products that have real value. The main components of intellectual capital are the human capital (managers and employees education, skills, experiences, trainings etc.), the structural capital (licenses, patents, copyrights, software, databases, organizational culture, organizational structure etc.) and the relational capital (relations with consumers, distributors, suppliers, investors, trademark, brand etc.). Each of these elements of intellectual capital contributes significantly to the success of the modern organization.

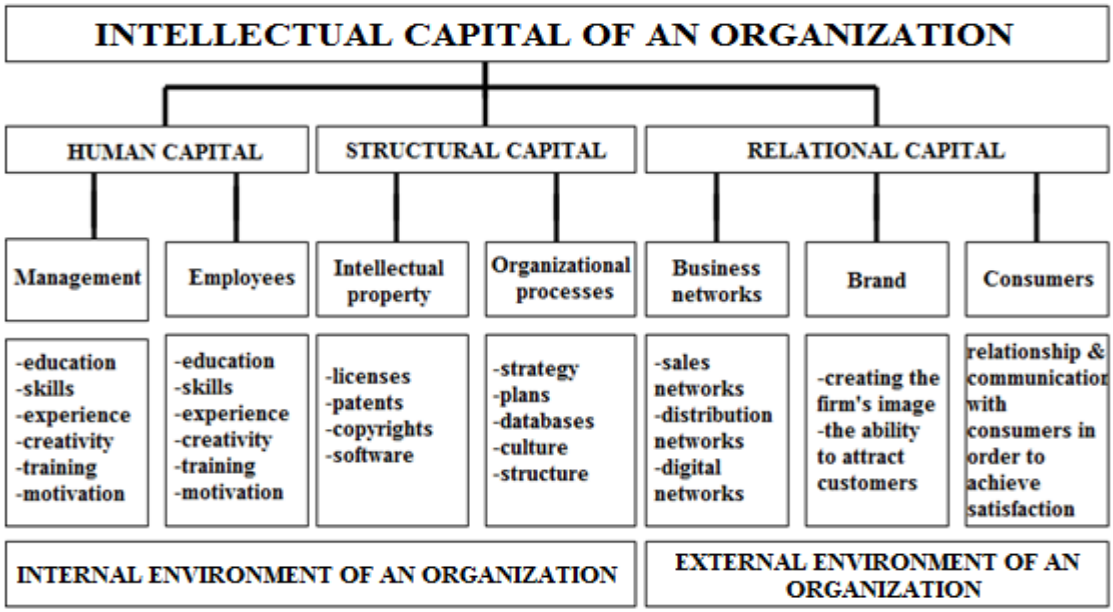

Figure 1: The intellectual capital structure of a modern organization [5]

The essence of an organizational intellectual capital lies in the value creation process. Value in an organization can be created when human capability (human capital) creates new business processes (structural capital), resulting in better products for consumers and increasing their loyalty (relational capital). Moreover, the interaction between the three constituent elements of intellectual capital is unique and unlike the usual material goods, the nature of intellectual capital is characterized by the synergistic effect. Hence, modern organizations must invest a huge effort in designing an appropriate information systems infrastructure that will be a significant motivator for creating an organization based on intellectual capital.

The importance of the intellectual capital for the modern organizations can be observed from another point of view as well. Namely, technological progress happens because organizations or individual inventors, in the desire to maximize profits, search for new and better discoveries. The opportunity to make a profit is what makes companies and entrepreneurs develop the computer, or produce a handheld camera, or produce calorie-free ice cream. Patents, copyrights, trademarks, etc., are legal mechanisms that guarantee the inventor a monopoly profit for a certain period of time. Without such mechanisms for the protection of intellectual property, it would be difficult to ensure the motivation of organizations and entrepreneurs for research work and development. So, it should be taken into consideration the fact that intellectual property, as a part of intellectual capital, is an

important determinant for the development of the modern organizations. In addition, the market value of the organization can be easily undermined if intellectual capital is not properly protected.

3. Previous work

The research detailed in this study builds upon a decade of work that explores the role of cloud services in supporting the daily operations of corporate entities, particularly in protecting intellectual capital [2][6][7][8][9][10][11]. A primary focus across these studies has been on key metrics like the Recovery Point Objective (RPO) and Recovery Time Objective (RTO), both of which serve as critical indicators of a data protection system's performance and reliability [12]. These parameters are especially relevant for intellectual capital protection, as they directly impact the continuity of access to vital knowledge assets during disruptions.

It is important to note that much of this research was conducted in simulated conditions, where key parameters were often derived from isolated environments, unaffected by other infrastructure elements. As such, the authors highlight that validating these results within a real-world production environment is essential to fully understanding their effectiveness in safeguarding intellectual capital.

4. Methodology

When evaluating outages and establishing recovery goals that align with organizational needs, it's essential to recognize that the process hinges on minimizing the time the organization is unable to operate. This process involves two key time-dependent elements. The first, a technical component, is the RTO, which defines the time required to restore systems, data, and network infrastructure. The second is Work Recovery Time (WRT), an organizationally focused measure that represents the time needed to fully reinstate operational processes.Together, these elements define the Maximum Tolerable Downtime (MTD), as outlined in the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). The MTD is calculated as the sum of RTO and WRT:

$$MTD = RTO + WRT \quad (1)$$

As shown in Figure 2, the RTO represents the duration needed to address technical recovery, while the remaining time up to the MTD is allocated to WRT, during which all information-based work processes are fully restored.

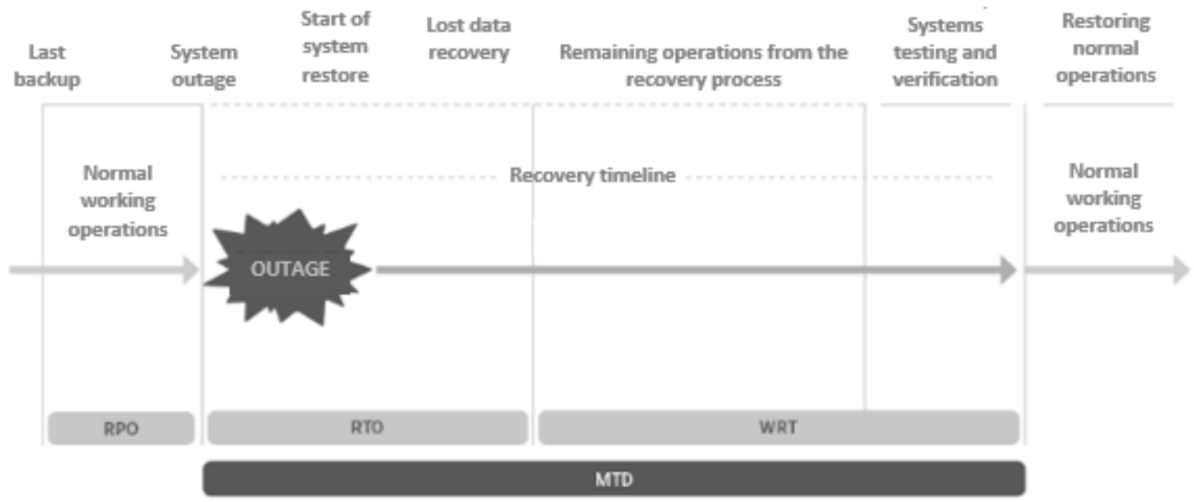

Figure 2: Maximum tolerable downtime in the context of intellectual capital protection

This approach not only ensures operational continuity but also plays a crucial role in protecting the organization's intellectual capital by minimizing downtime and safeguarding essential information systems.In the system design phase, defining requirements for data protection is crucial for ensuring information consistency and safeguarding intellectual capital. A key component in this process is the

RPO, which specifies the maximum age of data in backups at the time of recovery. As a time-dependent metric, the RPO indicates the point to which data will be restored, thus affecting potential data and information loss. This backward recovery process inevitably involves some data loss (except in cases of synchronous replication, where data loss can be eliminated). Consequently, organizations establish a Maximum Tolerable Data Loss (MTDL) threshold during sustainable business continuity planning to ensure data protection within acceptable loss limits. Systems designed to achieve zero data loss reveal an inverse relationship between RPO proximity to the outage and system cost: the closer the RPO, the higher the expense.

Using these parameters as a foundation, our research analyzed the performance and reliability of cloud-based recovery systems following outages. This analysis provides a parametric framework to guide the selection and implementation of recovery systems. By balancing technical, organizational, and financial considerations, this framework assists organizations in making informed choices to protect their intellectual capital, maintain operational continuity, and optimize recovery processes in alignment with business continuity objectives.

4.1. Production environment

This section outlines the working environment for the research, specifically describing the setup of a test virtual machine used to evaluate backup and recovery processes in a real-world, mission-critical environment. Given the need for stability and protection of intellectual capital, a dedicated server was configured as a virtual machine to monitor backup and restoration processes, utilizing cloud-based storage as a Recovery Service. For this purpose, Microsoft Azure was chosen as the cloud service provider, with the Microsoft Azure Recovery Service (MARS) [13] deployed to secure a single virtual machine (VM). Unlike the Disaster Recovery (DR) system discussed in [10], where Backup as a Service (BaaS) is implemented within a data center, our research focuses entirely on a cloud-deployed solution.

The data center supporting the research environment is illustrated in **Figure 3**.

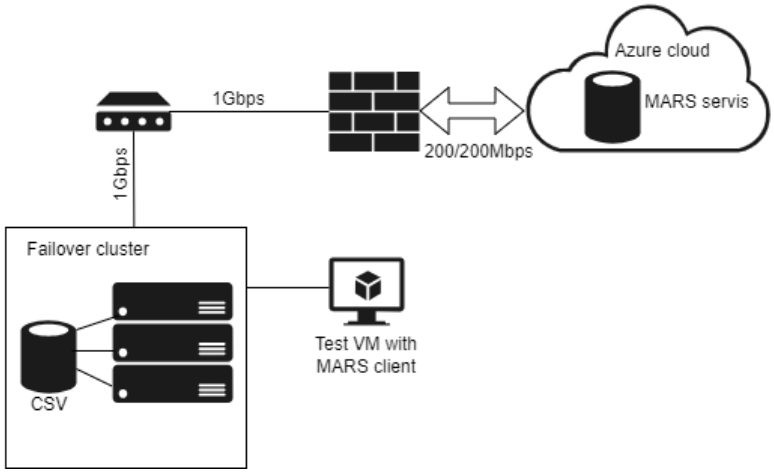

Figure 3: Data Center research environment

This production environment comprises three server systems, each with high fault tolerance across network, data, power, and storage components. The servers, running Windows Server 2019 with Hyper-V, form a virtual cluster that provides a failover mechanism, ensuring high availability (HA) for virtual systems [14]. This cluster-based setup enhances data center availability and service reliability, both locally and across the organization's network.

Due to the data center's strict adherence to operational continuity standards, availability and reliability are considered maximal, consistent with operational uptime goals. Performance success is validated through security and operational logs from the data center systems and Azure services. Microsoft Azure, the cloud provider used in this setup, boasts an impressive availability of nearly

100% (99.999999999% or 11 nines), underscoring its suitability for safeguarding critical information and ensuring uninterrupted access to the organization's intellectual capital.

4.1.1. Parametric prerequisites as a starting point for the research

In defining the key parameters as a starting point for evaluating the solutions in our research, it is essential to recognize that these parameters, from a technical perspective, directly influence the RPO and RTO, two critical metrics for assessing the effectiveness of data protection strategies [12]. Given that the analysis involves dynamic systems where parameter characteristics fluctuate based on operating conditions, it is necessary to consider some parameters as averages. During backup and restore operations, multiple factors, such as data packet delays and fluctuating network traffic, affect these values. The selection of parameters for analysis hinges on the specific objectives of the evaluation, guided by a Business Impact Analysis (BIA). This foundational analysis identifies the crucial parameters for determining the most appropriate recovery solution (primarily RPO and RTO) that align with the organization's needs. By defining these key parameters, organizations can make informed decisions to protect their intellectual capital, ensuring that data recovery strategies are both resilient and responsive to operational demands.In that context, the parametars that are incuded in creation of a BIA frame, in our research are taken as a basis for the creation of the concept of protection in company's intellectual capital:

- **LAN speed** - 1Gbps
- **Internet connection speed** - 200/200Mbps
- **Backup frequency** - daily
- **RPO** - ≤ 7 days
- **RTO** - ≤ 24 hours
- **Retention time of backup copies** – 7 days

4.2. System dynamics modeling aproach for the cloud-based system

Figure 4 illustrates the model of the cloud-based system, highlighting four derived components: two related to backup creation, one to data recovery, and one to the monthly cost of using a fully cloud-based service.

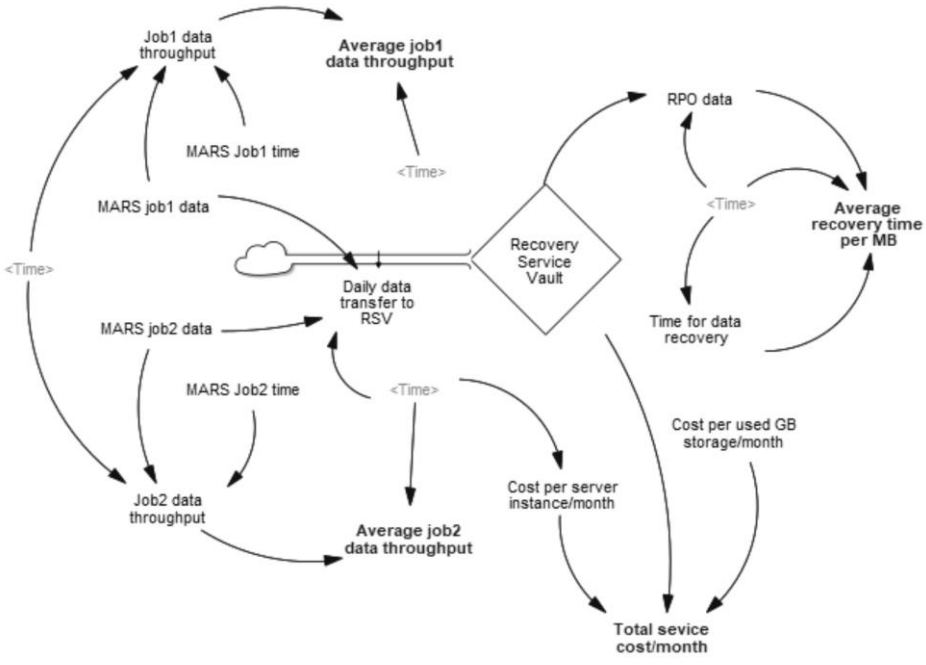

Figure 4: System dynamics model of cloud-based protection system

In the MARS concept, the data backup process involves two key steps, referred to as *job1* and *job2*. In the first step, an agent generates a backup of the virtual machine's system state, capturing essential configuration and operational data. In the second step, a comprehensive backup of remaining data, not covered in the initial step, is performed. This two-step process ensures a thorough safeguard of both system-critical data and broader informational assets, reinforcing the protection of an organization's intellectual capital by securing all facets of the virtual environment. Because of this backup/recovery concept, the model includes **Average job1 data throughput** and **Average job2 data throughput**, which represent the average amount of data transferred to the system's backup storage (Recovery Service Vault - RSV). The variable **Average recovery time per MB** reflects the time needed to recover 1 MB of data from the protective storage located in cloud, while **Total service cost/month** represents the ongoing expense of using cloud-based storage services. This four components are derived from the data captured with MARS agent instaled in the protected VM that are refered to the backup/recovery process.

The backup and recovery processes span eight time points. Seven points cover the backup policy cycle, while the final point captures the change in data volume within the recovery vault at the end of a 7-day cycle. Table 1displays the variable states in the model, showing changes over the specified timeframe, with a separate section summarizing the final values of derived components following the simulation based on the specified input parameters.

By tracking these parameters, organizations can make data-driven decisions on backup and recovery strategies to ensure robust protection of intellectual capital while maintaining cost-efficiency in a cloud environment.The values obtained from the simulation, as presented in Table 1, form the foundation for evaluating system performance under extreme data component conditions. These derived component values directly influence system performance and provide critical insights into how well the system can manage variations. By analyzing these impacts, organizations can better assess the system's capacity to protect intellectual capital, ensuring that backup and recovery processes remain resilient and effective even when subjected to demanding data loads.

Table 1:
Value states of the variables in the model

Variable	Value							
	1	2	3	4	5	6	7	8
Data backup process								
MARS job1 data (MB)	8362	8409	8463	8516	8569	8622	8678	
MARS Job1 time (sec)	3270	2993	3025	3110	2976	3105	3307	
Job1 data throughput (MB/s)	2.55719	2.80956	2.79769	2.73826	2.87937	2.77681	2.62413	
MARS job2 data (MB)	353	375	478	553	551	394	780	
MARS Job2 time (sec)	351	365	489	628	232	358	387	
Job2 data throughput (MB/s)	1.0057	1.0274	0.977505	0.880573	2.375	1.10056	2.0155	
Daily data transfer to RSV (MB)	8715	8784	8941	9069	9120	9016	9458	
Data recovery process								
RPO data (MB)								7690
Time for data recovery (sec)								1380
Derived variables								
Average job1 data throughput (MB/s)								2.57731
Average job2 data throughput (MB/s)								1.83045
Average recovery time per MB (sec)								5.57246
Total sevice cost/month (dollars)								7.82701

To validate the system's performance in alignment with the requirements emphasized in the BIA, we added five new components to the model. These include two components (**Backup time Job1 (Test data)** and **Backup time Job2 (Test data)**) to calculate the time required for each backup creation step. Another component, **Recovery time (Test data)**, measures the data recovery duration. Additionally, **Test data** serves as a central component representing the total data volume held by the server system within the organization (set at 531 GB). The fifth component, **Total service cost/month (Test data)**, calculates the monthly service cost based on this data volume.These enhancements provide a detailed view of the system's performability, presented in the Table 2**:**

ensuring that it effectively supports the protection of intellectual capital by accommodating the organization's data recovery and backup needs within cost-effective parameters.

Table 2:
Simulation results of the model for a cloud-based system with Test data

Variable	Value
Derived variables	
Average job1 data throughput (MB/s)	2.57731
Average job2 data throughput (MB/s)	1.83045
Average recovery time per MB (sec)	5.57246
Test data simulation values	
Test data (MB)	531012
Backup time Job1(Test data) (hours)	57.2315
Backup time Job2(Test data) (hours)	80.5831
Recovery time (Test data) (hours)	26.47
Total sevice cost/month (Test data) (dollars)	43.7893

If we compare the results obtained from the validation process, with the values requested in the BIA, we will notice that they exceed the maximum allowed in the request of BIA (in the BIA the maximum allowed value for RTO is 24 hours).

5. Conclusion

The simulation and research conducted in this study highlight the critical role of cloud-based systems in enhancing business continuity through robust data backup and recovery mechanisms. By thoroughly evaluating the Microsoft Azure Recovery Service - MARS model, we explored how cloud storage solutions can sustain organizational resilience, particularly in scenarios that require immediate data access and rapid recovery. This approach proves essential for safeguarding an organization's intellectual capital, as it ensures continuous access to critical information and assets that form the backbone of organizational knowledge and competitive advantage.

The simulation validates the effectiveness of cloud-based systems in enhancing resilience and protecting intellectual capital. Cloud solutions, exemplified by the MARS model, enable organizations to maintain continuity and safeguard their information assets against disruptions. The insights gained from this study provide a framework for evaluating cloud-based backup and recovery systems, focusing on achieving optimal RTO and RPO, scalability, and cost efficiency. Due to the wide time frame of the cloud-based system in the data recovery processes, such systems are extremely useful and widely applicable for the recovery of systems that do not have critical importance for the business operations of companies or are used as an archive to store a large amount of data or documents for a long period of time. Ultimately, organizations that prioritize intellectual capital protection through robust data management strategies are better positioned to sustain competitive advantage and support long-term growth. The shift towards cloud-based solutions for intellectual capital protection, therefore, represents a strategic imperative in today's data-driven business landscape.

References:

[1] A. Mathew, C. Mai, "STUDY OF VARIOUS DATA RECOVERY AND DATA BACK UP TECHNIQUES IN CLOUD COMPUTING & THEIR COMPARISON", 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology, 2018, Bangalore, India

[2] A.A. Tamimi, R. Dawood, L. Sadaqa, "Disaster RecoveryTechniques in Cloud Computing", IEEE Jordan InternationalJoint Conference on Electrical Engineering and InformationTechnology (JEEIT), 2019, Amman, Jordan.

[3] S. Shahzadi, G. Ubakanma, M. Iqbal, T. Dagiuklas,"Autonomous, Seamless and Resilience Carrier Cloud BrokerageSolution for Business Contingencies During Disaster Recovery",IEEE 20th International Conference on High PerformanceComputing and Communications, 2018, Exeter, UK.
[4] T. Wood, E. Cecchet, K. Ramakrishnan, P. Shenoy, J. Van DerMerwe, A. Venkataramani, "Disaster recovery as a cloud service:Economic benefits & deployment challenges", 2nd USENIXWorkshop on Hot Topics in Cloud Computing, 2010, Boston.
[5] Sundać Dragomir, Švast Nataša, "Intelektualni kapital-temeljni čimbenik konkurentnosti poduzeća", Ministarstvo Gospodarstva, Rada i Poduzetništva, Zagreb, 2009, pp. 37.
[6] A.Mishra, V.Sharma, A.Pandey, "Reliability of CloudComputing Services", IOSR Journal of Engineering, Volume:04,Issue:01, pp.51-60, 2014.
[7] A.Mishra, V.Sharma, A.Pandey, "Reliability, Security andPrivacy of Data Storage in Cloud Computing", InternationalJournal of Advanced Research in Computer Science, Volume 5,No.3, 2014.
[8] H.B.Rebah, H.B.Sta, "Disaster Recovery as a Service: A DisasterRecovery Plan in the Cloud for SMEs", Global Summit onComputer & Information Technology, 2016, Sousse, Tunisia.
[9] J.Mendonça, R.Lima, E.Andradey, J.Araujoy, D.S.Kim,"Multiple-criteria Evaluation of Disaster Recovery StrategiesBased on Stochastic Models", 16th International Conference onthe Design of Reliable Communication Networks (DRCN),IEEE, 2020.
[10] J.Mendonca, R.Lima, E.Queiroz, E.Andrade, D.S.Kim,"Evaluation of a Backup-as-a-Service Environment for DisasterRecovery", IEEE Symposium on Computers andCommunications (ISCC), 2019, Barcelona, Spain.
[11] J.Mendonca, R.Lima, R.Matos, J.Ferreira, E.Andrade,"Availability Analysis of a Disaster Recovery Solution ThroughStochastic Models and fault enjection experiments",32ndInternational Conference on Advanced Information Networkingand Applications, IEEE, 2018.
[12] S. Nikolovski, P. Mitrevski, “On the Requirements for SuccessfulBusiness Continuity in the Context of Disaster Recovery”, Proc.of the 57th International Scientific Conference on Information,Communication and Energy Systems and Technologies (ICEST),Ohrid, North Macedonia, 2022.
[13] B. Chakraborty, Y. Chowdhury, "Introducing Disaster Recoverywith Microsoft Azure: Understanding Services and Tools forImplementing a Recovery Solution", Apress, 2020.
[14] N.Dhanujati, A.S.Girsang, "Data Center-Disaster RecoveryCenter (DC-DRC) For High Availability IT Service",International Conference on Information Management andTechnology (ICIMTech), 2018, Jakarta.