РЕПУБЛИКА МАКЕДОНИЈА
УНИВЕРЗИТЕТ „ СВ. КЛИМЕНТ ОХРИДСКИ “– БИТОЛА
ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ
И КОМУНИКАЦИСКИ ТЕХНОЛОГИИ – БИТОЛА

Сашо Николовски

АНАЛИЗА НА НАДЕЖНОСТА И ПЕРФОРМАНСИТЕ НА КЛАУД-БАЗИРАНИ СИСТЕМИ ЗА ОПРАВУВАЊЕ ОД КАТАСТРОФИ

- Авторезиме на докторска дисертација -

Битола, 2023

ЧЛЕНОВИ НА КОМИСИЈАТА ЗА ОЦЕНКА И ОДБРАНА НА ДОКТОРСКАТА ДИСЕРТАЦИЈА

Д-Р ПЕЦЕ МИТРЕВСКИ
РЕДОВЕН ПРОФЕСОР
ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ И КОМУНИКАЦИСКИ ТЕХНОЛОГИИ
УНИВЕРЗИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“- БИТОЛА

Д-Р БЛАГОЈ РИСТЕВСКИ
РЕДОВЕН ПРОФЕСОР
ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ И КОМУНИКАЦИСКИ ТЕХНОЛОГИИ
УНИВЕРЗИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“- БИТОЛА

Д-Р НИКОЛА РЕНДЕВСКИ
ВОНРЕДЕН ПРОФЕСОР
ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ И КОМУНИКАЦИСКИ ТЕХНОЛОГИИ
УНИВЕРЗИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“- БИТОЛА

Д-Р САШО ЈОСИМОВСКИ
РЕДОВЕН ПРОФЕСОР
ЕКОНОМСКИ ФАКУЛТЕТ
УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ“- СКОПЈЕ

Д-Р БОЖИДАР МИЛЕНКОВСКИ
РЕДОВЕН ПРОФЕСОР
ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ НАУКИ И КОМПЈУТЕРСКО ИНЖЕНЕРСТВО
УНИВЕРЗИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“- БИТОЛА

Во современото опкружување на секоја компанија чие работење е базирано на информатички технологии, се јавува потребата од донесување на план за одржување на непрекинатост во работењето, во кој е вграден план за оправување од катастрофи чија цел е обезбедување на услови и процедури за брзо закрепнување во случаи по настанат испад. Поттикнати од овие два аспекти за одржување на информациските системи и нивните информатички платформи, гледајќи ја областа за оправување по настанат испад или катастрофа посебно интересна и предизвикувачка за истражување, во рамки на дисертацијата е направена компаративна анализа на системи за оправување со посебен акцент ставен на системите кои делумно или целосно се поставени во облак и нивната надежност за сигурно и безбедно извршување на улогата која ја имаат во целокупното сценарио. Имајќи ја предвид актуелноста на сервисите за заштита и оправување на податоци и информациски системи поставени во облак, за потребите на истражувањето, во реална продукциска околина, се имплементирани два системи за заштита и оправување.

Со цел идентификување на вредностите на клучните параметри според кои би се оценувала нивната перформабилност и надежност во зададени реални услови на нивна работа, во истражувањето е користен софтвер за симулација за подобрување на перформансите на реалните системи и притоа е изведена System Dynamics анализа за секој од разгледуваните системи. Во таа насока, во трудот се прави идентификација на рамка со параметрите според кои би се правел избор на решение за заштита и оправување на податоците и информациските системи во организациските структури. Придобивките од вака предложената рамка се однесуваат пред сè на детерминирање на пристапот и фазите при селекција и избор на соодветно решение за заштита и оправување на податоците и информациските системи, преку можноста за приспособување на избраниот концепт кон опкружувањето, согласно зацртаните временски рамки поставени во планот за деловен континуитет и планот за оправување од настанат испад.

Со спроведените анализи и изведените заклучоци од нив, се дава директен придонес кон правилното размислување за носење на одлуки при изборот на концепти за изведба на системи за оправување по настанат испад или катастрофален прекин, во зависност од потребите на субјектите кои истото го имплементираат.

1 ОБЈАВЕНИ ТРУДОВИ ПОВРЗАНИ СО ИСТРАЖУВАЊЕТО

Трудови во зборници на научни трудови презентирани на меѓународни академски собири:

1. S. Nikolovski, P. Mitrevski, "On the Requirements for Successful Business 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
2. S. Nikolovski, P. Mitrevski, "Data protection and recovery performance analysis of cloud-based recovery service", Proc. of the 58th International Scientific Conference on Information, Communication and Energy Systems and Technologies ", Nis, Serbia, 2023

Трудови во меѓународни научни списанија:

1. S. Nikolovski, P. Mitrevski, "Modelling and simulation of data protection systems for business continuity with disaster recovery", submitted for publication in International Journal of Business Continuity and Risk Management (under review)

2 ПРЕДМЕТ И ЦЕЛ НА ИСТРАЖУВАЊЕТО

Постојаната достапност на компаниските информациски системи за многумина наметнува впечаток и мислење дека деловниот континуитет може да се толкува или разбере како заштита на идното деловно и функционално опстојување на организацијата од некаква форма на нарушување.

Кај современите работни процеси кои се базирани на дигитални системи, нултиот застој при оперативно нарушување разгледувано од аспект на одржана деловност, е идеален исход за сите организации. Ваквото очекување не е секогаш можно или реално остварливо од бројни причини (испади поради временски непогоди, сајбер напади и сл.) и покрај достапноста на бројни решенија за заштита и оправување како во локалните податочни центри на организациите, така и решенија базирани на користење систем во облак [3]. Затоа, од аспект на управување со ваквите организации, се повеќе се посветува внимание на намалување на влијанието од испадите врз целокупниот работен процес преку проценка на максималното време на испад кој самата организација може да си го дозволи, без притоа да има трајни последици по нејзиното понатамошно работење.

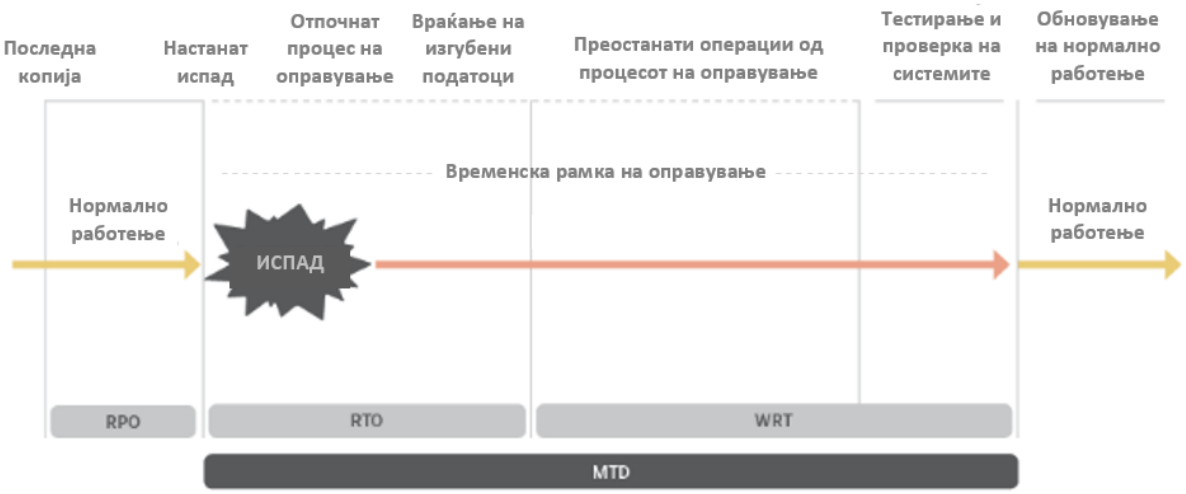
При анализа на испадите и поставување на целите за конзистентно оправување од нив, а притоа истото да биде прифатливо за организацијата, може да се забележи дека целиот процес се базира пред сè на времето во кое организацијата е надвор од оперативност и притоа во себе опфаќа два временски зависни елементи.

Едниот елемент е одреден од системскиот или технолошкиот аспект прикажан преку целното време на оправување (Recovery Time Objective-RTO), а другиот, кој е повеќе организациски ориентиран, го претставува потребното време за целосно оперативно враќање на работните процеси (Work Recovery Time-WRT).

Овие две временски компоненти од процесот на оправување го одредуваат максималното толерантно време на испад (Maximum Tolerable Downtime-MTD) кое е предвидено со плановите за деловен континуитет и планот за оправување од катастрофи и претставува збирно време од целното време на оправување и потребното време за оперативно враќање на работните процеси:

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

Ова значи дека RTO како параметар е временски интервал во кој се прави оправување на работењето во техничко-технолошкиот дел на организацијата, време во кое се враќаат системите, податоците и мрежната инфраструктура. Преостанатото време до максималното толерантно време на испад е времето за оперативно враќање на работните процеси (WRT) и во него се врши оправување на сите работни процеси кои се базираат на информатичките и информациските системи (Слика 1).



Слика 1 *Максимално толерантно време на испад*

Временската рамка за оправување која е ограничена со рамката во која е поставено MTD, во себе вклучува и неколку компоненти кои се составен дел од овој процес. Овие компоненти имаат за цел враќање на податоците од нивната сигурносна копија (backup) која е временски најблиску до настанатиот испад, спроведување на последователни операции како финален дел на оправувањето и секако, проверка и тестирање на функционалноста на системите пред нивно официјално ставање во функција за воспоставување на нормалното работење.

При дефинирање на потребите, во фазата на дизајнирање на системот, компонентата која е директно поврзана со податоците, а со тоа и со конзистентноста на информациите, е целната точка на оправување (Recovery Point Objective-RPO). Овој параметар е временски зависен и ја дава „староста“ на податоците во сигурносната копија поставена во временската точка од која ќе се прави нивно враќање во системите за оперативна употреба. Имајќи предвид дека RPO процесот на враќање е враќање на податоци од минато време (backward recovery), загубата на податоци и финални информации е неминовна (освен во ситуации на синхрона репликација каде загубата на податоци е нула). Затоа, при проектирање на системите во рамки на планирањето на одржливиот деловен континуитет, зададен е максималниот праг на толерантност од загуба на податоци кои организацијата може да си го дозволи (Maximum Tolerable Data Loss-MTDL). Системите кои овозможуваат нулта загуба на податоци создаваат обратно-пропорционална врска на количеството на изгубени податоци при процесот на оправање со цената на чинење на системите. Ова значи дека колку е поблиску RPO до моментот на појава на прекин, толку е цената на чинење на ваквите системи повисока и обратно.

Од таа причина, користејќи ги гореспоменатите временски компоненти како појдовни, во рамки на трудот се спроведе анализа на перформансите и надежноста на два

системи за оправување по настанат испад, со цел добивање на параметарска рамка за избор и поставување на системи кои ќе ги задоволат барањата на организациите при процесите на оправување од техничко-технолошки, организациски и финансиски аспект кој многу често има пресудно влијание при правење на конечниот избор.

При спроведување на истражувањето, целокупниот процес опфати низа активности кои се состојат во:

1. Изработка на детален проект, поставување и конфигурирање на податочен центар со вклучена податочна заштита базирана на хардверски уред DellEMC DP4400, како решение поставено во место и Microsoft Azure Recovery Services (MARS) како решение целосно поставено во облак,
2. Инсталирање и конфигурирање на системите за податочна заштита за потребите на истражувањето. Бројот на примероците на временските и податочните параметри преземени од системите беше усогласено со вредностите предвидени со анализата на деловното влијание на испадите (Business Impact Analysis-BIA) и минималниот број на примероци поддржан од системите за заштита (14 дена од хибридниот систем и 7 од системот поставен во облак).
3. После временски период од една година (декември 2021-декември 2022) во кој системите имаа континуирана оперативност, изведена е анализа за нивното работење со преземање на податоците за временските и податочните параметри од изведување на операциите за заштита (backup) и оправување (recovery/restore) на податоците, при што се утврдени параметрите кои треба да се калкулираат од вредностите на параметрите преземени од системите за заштита,
4. За секој од разгледуваните системи се изработени по два модели – еден основен модел, во кој со користење на преземените вредности за временските и податочните параметри од системите се добиени вредности за утврдените изведени параметри во моделот и еден проширен модел, во кој со користење на вредностите на изведените параметри од основниот модел се калкулирани вредности за перформансите на системите со зададено тестно количество податоци во разгледувана оперативна средина. При изработката на моделите, изработен е и модел за надежност на системите за чие калкулирање се користени временски рамки согласно поставувањата направени во системите,
5. Направена е компаративна анализа на добиените резултати од симулациите на моделите за двата системи и изведени се заклучоци врз база на кои во завршниот текст на дисертацијата се дадени препораки за правилно димензионирање и поставување на различните концепти за заштита во различни ситуации на употреба.

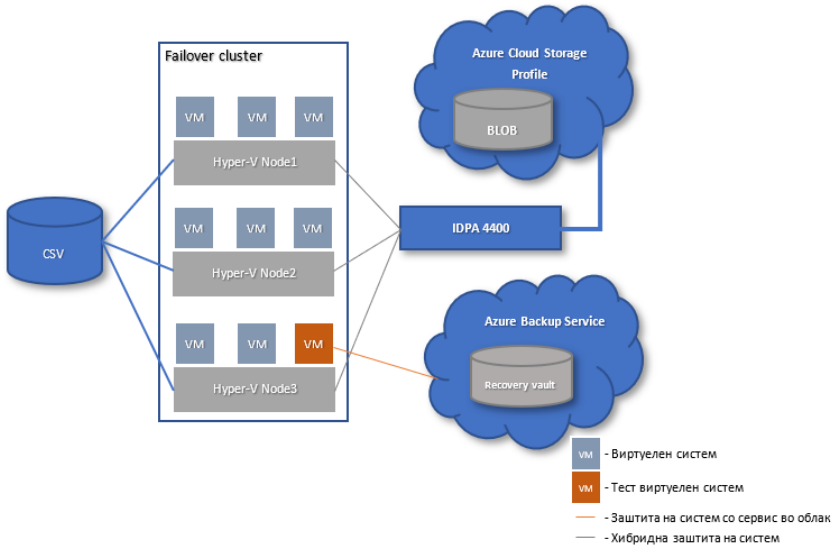
Според сè погоре наведено, фокусот на истражувањето е поставен во областа на одржување на деловниот континуитет во работењето на компаниските субјекти, а анализата на надежноста и перформансите на системи за оправување од катастрофи се наметна како предмет на истражување, при што целта во него е поставена на градење параметарска рамка која ќе даде прецизни насоки при вршење на избор на системско решение за заштита и оправување на податоци и информациски системи во податочните центри.

3 ГЛАВНИ ПРИДОБИВКИ

Истражувањето опфатено во текстот на дисертацијата е засновано на низа текстови произлезени од истражувачката работа во изминатиот период од десетина години, период во кој клауд сервисите добија на актуелност во секојдневното работење на компаниските субјекти [4][7][8][20][26][27][28]. Во интересот на овие истражувања постојано циркулираат неколку целни параметри од кои како заеднички се забележуваат расположливоста (availability), целната точка за оправување на податоците (RPO) и целното време за нивно оправување (RTO), како параметри директно зависни од перформансите на системите за податочна заштита и нивната надежност.

Во пракса, за применливоста на методите и алгоритмите развиени во посочените истражувања кои беа искористени како појдовна основа за спроведеното истражување во дисертацијата, од страна на авторите е посочено дека сепак во најголем дел ваквите истражувања се направени во услови на симулација со најчеста примена на вредности на клучните параметри добиени во изолирана средина, односно без влијание од околината во која истите се наоѓаат, а како потврда за нивната применливост, потребна е нивна валидација добиена од нивна практична примена во продукциска средина.

Наспроти системите и концептите кои се користени во овие истражувања, системите кои се искористени во истражувањето на дисертацијата се поставени во продукциски податочен центар (Слика 2).



Слика 2 *Продукциски податочен центар - блок шема*

Имајќи предвид дека истражувањето се спроведува во реална работна околина со исклучителна важност за постојаност на функционалноста на сите системи во неа, за потребите на истражувањето е поставен засебен серверски систем како тест виртуелна машина која беше искористена за следење на процесите за податочна заштита (backup) и оправување (recover/restore) во рамки на двата системи за заштита кои кај себе вклучуваат заштитни складишта поставени во облак. Во насока на утврдување на перформабилноста на системите за податочна заштита, во рамки на истражувањето, се развија два основни и два проширени модели во кои со симулација на оперативноста на реалните системи се добија вредности за целните параметри кои се од интерес за изведување на заклучоците. Практичната имплементација на системите кои се користат во истражувањето, опфаќаат примена на хибридно решение (хардверски уред со складишно ниво за податоци поставено во облак) поставено во податочниот центар, со инсталиран Avamar софтверски агент во серверскиот систем кој е предмет на податочна заштита и решение целосно базирано на клауд-технологија Microsoft Azure Recovery Service (MARS), со инсталиран MARS агент во серверскиот систем. При изработката на сигурносните копии од податоците со помош на хибридното решение, сигурносната копија првично се чува во локалното складиште на уредот за временски период кој е претходно поставен, за по истекот на тој период копијата да биде префрлена во складишното ниво поставено во облак за долготрајно нејзино чување. Во случајот со изработка на сигурносните копии со помош на MARS агентот, сигурносните копии се поставуваат и чуваат директно во складиштето поставено во облак, со однапред поставен период на чување.

3.1 Модели, симулација и резултати

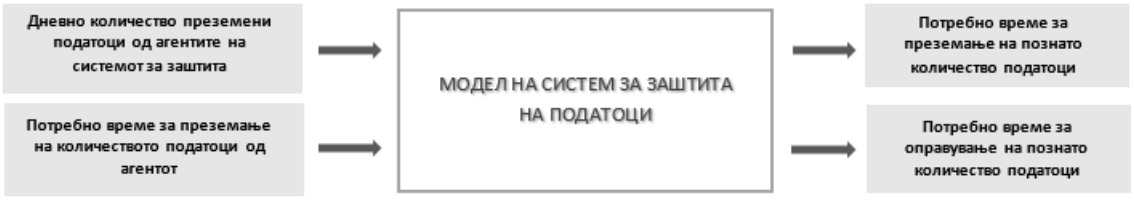
При поставување на моделите за користените заштитни системи во истражувањето, главниот акцент во нив е ставен на времињата за извршување на операциите за правење сигурносна копија и времињата за враќање на податоците од нив. Она што е значајно за изработените модели е дека во нив како извор за влезните вредности на променливите се користат вредностите преземени од реалните системи. Иницијалните вредности за количествата податоци се преземени од агентите, за временски примерок од 14 дена во случајот со хибридниот систем и 7 дена во случајот на системот поставен во облак, со цел да се опфати истекот на копиите, но и да се прикаже врската на складиштата во облак со условите поставени во податочниот центар за префрлањето на податоците кон нив. Како појдовна точка според која се одредени параметрите земени при поставување на моделите е анализата на деловното влијание на испадите (BIA), имплементирана во рамки на политиките за заштита во податочниот центар, а вредностите кои се поставени како целни, се дадени во Табела 1 каде е направено издвојување на вредностите по одредени параметри за секој од системите посебно.

Во табелата, за хибридниот систем е наведен Avamar агентот кој е поставен во серверскиот систем за кој се прават сигурносни копии, а за системот во облак наведен е MARS агентот.

Агент	Честота на правење копии	Време на задржување на копија	Точки за оправување	Политика за префрлување во облак	RPO	RTO
Avamar	дневно	14	7+7+60	> 14 дена	≤ 7 дена	≤ 5 часа
MARS	дневно	7	2*7+3	/		

Табела 1 *Поставени параметри во BIA*

Сценариото за правење на сигурносни копии е целосно усогласено со вредностите дадени во Табела 1, а за следење и оценка на процесот за враќање на изгубени податоци од избрана временска точка за оправување (RPO), направена е симулација на оштетување (бришење) на папки со документи, на кои е извршен процес на оправување. На Слика 3, во општа форма, се прикажани влезно-излезните параметри во моделите на двата разгледувани системи.



Слика 3 *Влезно-излезни параметри на моделите*

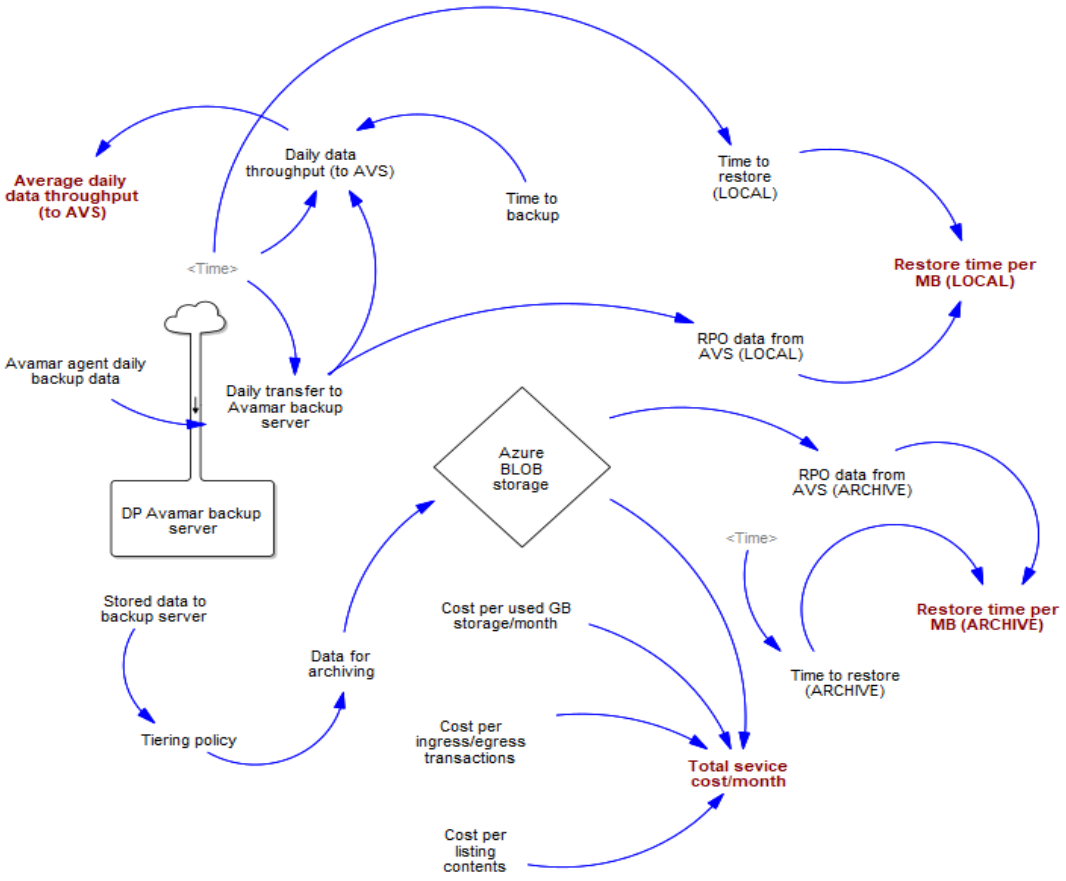
Од приказот може да се забележи дека како влезни параметри за двата модели се поставени количеството податоци пренесено на дневно ниво во заштитните складишта на системите и времето за кое истите се пренесени во складиштата на заштитните системи. Како излезни параметри од моделите се дефинирани изведени параметри за времето потребно за заштита на зададено количество податоци и времето за негово оправување во рамки на системот кој е предмет на заштита. При изработката на моделите за двата системи, првично се поставени основните модели кои во себе опфаќаат низа променливи поврзани помеѓу себе со релации преку кои ги менуваат состојбите на резултантните компоненти и складишните системи во нивните концепти. За утврдување на перформабилноста на системите при заштита и оправување на големи количества податоци, за секој од системите е поставен проширен модел во кој се додадени дополнителни компоненти преку кои се добиени конкретни вредности за временските параметрите кои се однесуваат на процесите за изработка на сигурносни копии и оправување на податоците.

3.1.1 Модел на хибриден систем

Основниот модел на хибридниот систем е прикажан на Слика 4 каде се појавуваат четири изведени компоненти со кои е опфатен процесот на изработка на сигурносни копии од податоците, како и процесот за оправување при настанато оштетување на истите. Временската рамка во која се одвива процесот на симулација во дадениот модел е усогласена со BIA каде процесот на изработка на сигурносни копии се одвива во 14 временски термини, а процесот за оправување на податоците и нивното преместување во складишното ниво поставено во облак е поставено во еден термин последователен по временската рамка за изработка на сигурносните копии.

Вредностите на променливите во основниот модел се прикажани во Табела 2 со посебни прикази на компонентите од процесот за изработка на сигурносните копии (backup process), процесот за оправување (restore process) и вредностите на изведените променливи во моделот.

На Слика 5 е даден графички приказ на состојбите на влезните компоненти во моделот.

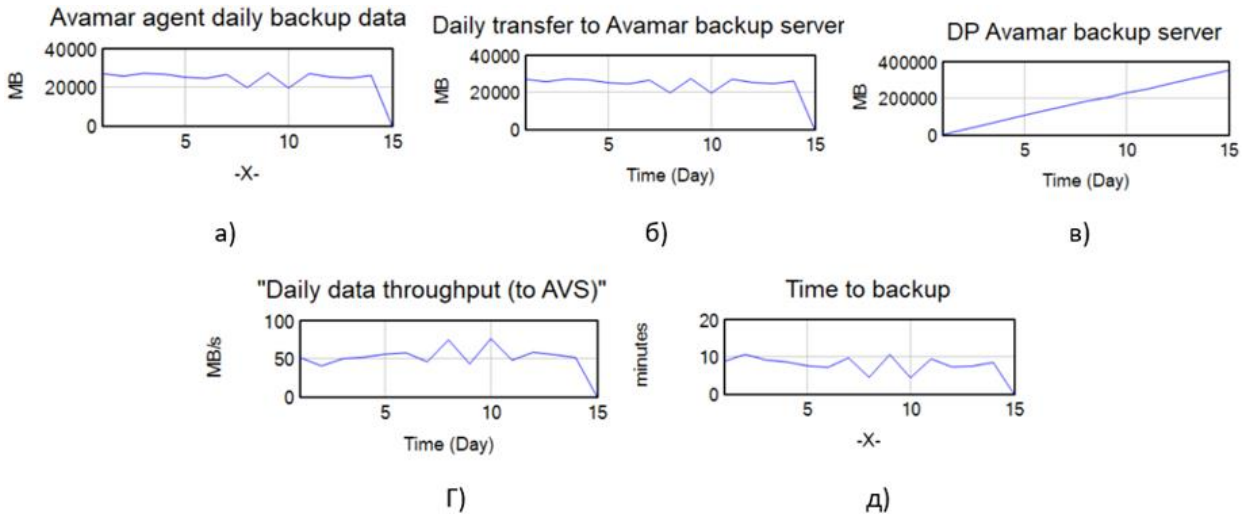


Слика 4 *Основен модел на хибриден систем со податочно ниво во облак*

Како изведени компоненти во моделот се појавуваат **Average daily data throughput (to AVS)**, изведена променлива која е добиена како средна вредност на количеството податоци пренесено до заштитното складиште во системот (Avamar backup server - AVS) од Avamar агентот во серверскиот систем, променливата **Restore time per MB (LOCAL)** која го прикажува потребното време за оправување на 1MB количество податоци преземено од локалното складиште на системот DP4400, **Restore time per MB (ARCHIVE)** променлива која го прикажува потребното време за оправување на 1MB количество податоци кои биле преместени во складишното ниво на уредот поставено во облак и секако, изведената променлива **Total service cost/month** која ги прикажува трошоците за користење на складишен сервис поставен во облак.

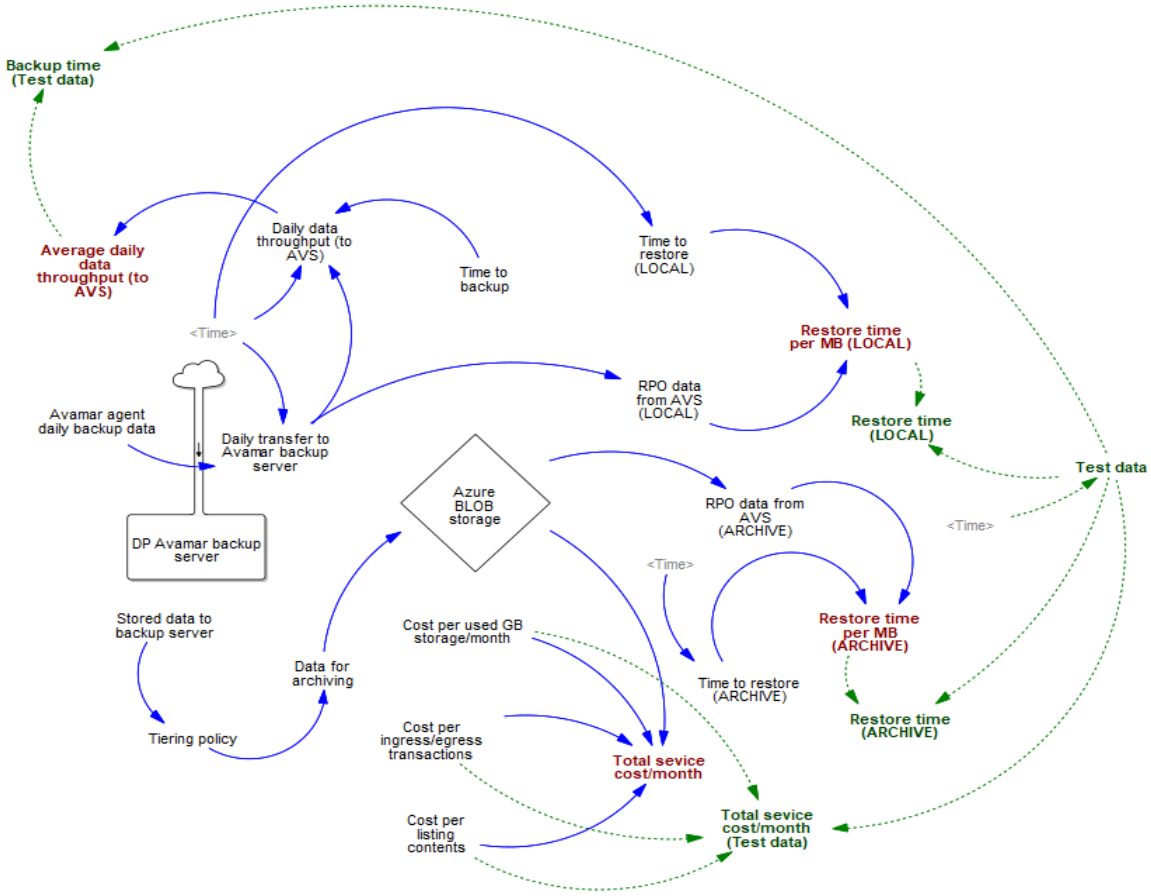
Variable	Value														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Data backup process															
Avamar agent daily backup data (MB)	26956	25712	27194	26710	25147	24520	26529	19711	27342	19574	27024	25262	24644	26082	
Daily transfer to Avamar backup server (MB)	26956	25712	27194	26710	25147	24520	26529	19711	27342	19574	27024	25262	24644	26082	
Daily data throughput (to AVS) (MB)	51.3448	40.3022	49.8059	51.8661	55.7633	57.5587	45.7428	74.6629	43.0596	76.1693	47.9149	58.3472	55.132	51.4438	
Time to backup (minutes)	8.75	10.633	9.1	8.583	7.516	7.1	9.666	4.4	10.583	4.283	9.4	7.216	7.45	8.45	
Data restore process															
RPO data from AVS (ARCHIVE) (MB)															1824
RPO data from AVS (LOCAL) (MB)														1824.01	
Time to restore (ARCHIVE) (seconds)															470.1
Time to restore (LOCAL) (seconds)														38.24	
Derived variables															
Average daily data throughput (to AVS)															54.2224
Restore time per MB (LOCAL) (seconds)															0.0209649
Restore time per MB (ARCHIVE) (seconds)															0.25773
Total sevice cost/month (dollars)															1.57912

Табела 2 *Вредности на променливите поставени во основниот модел*



Слика 5 *Графички приказ на состојбата на параметрите*

Согласно предметот и целите на истражувањето за утврдување на перформабилноста на решението, основниот модел на системот е надграден со пет нови компоненти кои немаат влијание на вредностите во основниот модел (Слика 6).



Слика 6 *Проширен модел на хибриден систем со податочно ниво во облак*

Од приказот на проширениот модел може да се забележат врските помеѓу изведените компоненти од основниот модел и дополнителните компоненти за зададено тестно количество податоци во проширениот модел. Како дополнителни компоненти во моделот се појавуваат компонентата **Test data** која го го внесува тестното количество податоци (531 GB), **Backup time (Test data)** како компонента во која се калкулира потребното време за изработка на сигурносна копија од зададено количество податоци, компонентите **Restore time (LOCAL)** и **Restore time (ARCHIVE)** во кои е калкулирано времето потребно за оправување на зададено количество податоци во случај кога процесот се изведува од локалното складиште на системот со RPO ≤ 14 дена или од нивото на складиштето поставено во облак каде 15 ≤ RPO ≤ 60 дена, како и компонентата **Total service cost/month (Test data)** која ги дава вкупните месечни трошоци за користење на складишниот сервис на системот поставен во облак. Вредностите на дополнителните компоненти поставени во проширениот модел на системот се прикажани во Табела 3 од каде може да се забележи дека некои од резултантните компонентите во проширениот

модел, повеќекратно ги надминуваат максимално дозволените вредности за нив предвидени во BIA, што ги прави некорисни за потребите на организацијата.

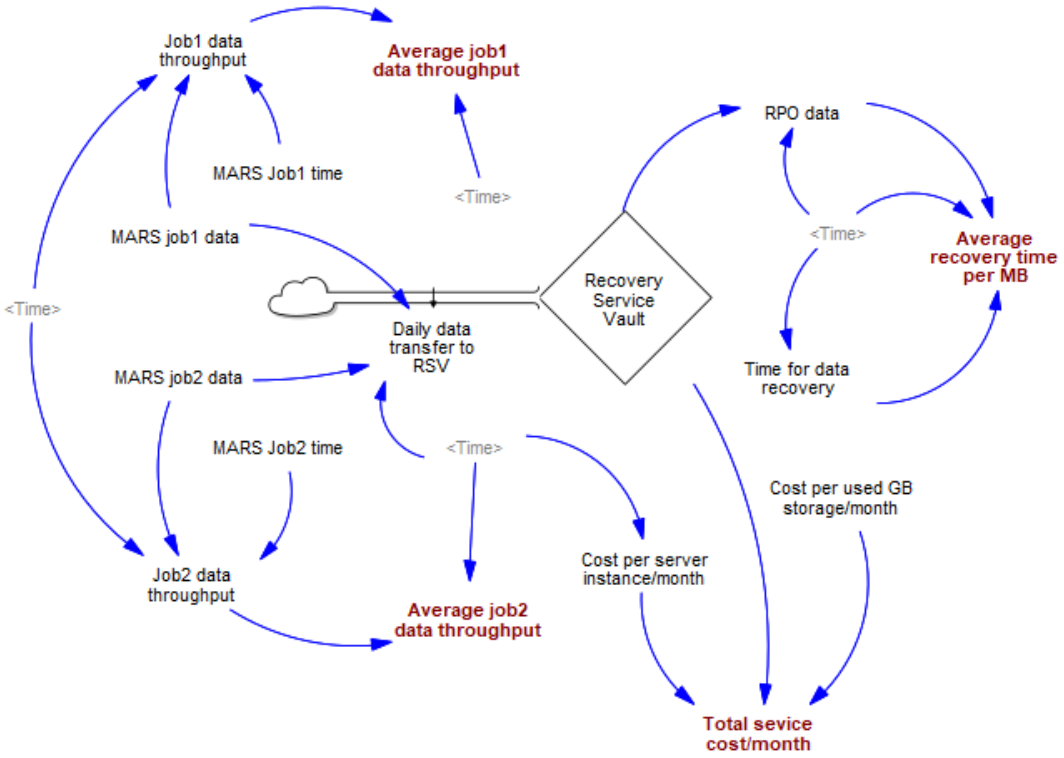
Variable	Value
Derived variables (basic model)	
Average daily data throughput (to AVS) (MB/s)	54.2224
Restore time per MB (ARCHIVE) (seconds)	0.25773
Restore time per MB (LOCAL) (seconds)	0.0209649
Test data simulation values (extended model)	
Test data (MB)	531012
Backup time (Test data) (hours)	2.72034
Restore time (ARCHIVE) (hours)	38.016
Restore time (LOCAL) (hours)	3.09239
Total sevice cost/month (Test data) (dollars)	11.6602

Табела 3 *Резултати од симулацијата на проширен модел за хибриден систем*

Конкретно, компонентата *Restore time from (ARCHIVE)* има многукратно повисока вредност (38 часа) од максималната вредност предвидена во BIA (≤5 часа) и затоа, нивото поставено во облак, во овој случај не би можело да се користи за брзо оправување на системите во организацијата и враќање на нејзината оперативност и функционалност на нивото од пред настанување на испадот. Наспроти оваа вредност, вредноста на компонентата *Restore time (LOCAL)* која изнесува 3 часа и 5 минути е во временската рамка предвидена во BIA, што укажува дека поставувањето на овој систем во структурата на податочниот центар може да ги задоволи поставените барања во анализата. Од аспект на создавање на сигурносна копија, вредностите на компонентата *Backup time (Test data)* целосно ги задоволуваат барањата за брза изработка на копиите во терминте предвидени за нивно спроведување. Треба да се има предвид дека ваквите системи имаат комплексна архитектура не само хардверски, туку и софтверски, каде преку низа алгоритми со текот на времето на користење, времето за кое ќе се изработуваат копиите може да биде драстично пократко од она што беше земено како средно време во основниот модел.

3.1.2 Модел на систем поставен во облак

Основниот модел на системот поставен во облак е прикажан на Слика 7 каде исто како кај хибридниот систем, се појавуваат четири изведени компоненти од кои две се однесуваат на процесот на изработка на сигурносна копија, една на процесот за оправување на податоците и една на месечните трошоци за користење на ваквиот сервис целосно поставен во облак.



Слика 7 *Основен модел на систем поставен во облак*

Приказот на компонентите од кои е изграден моделот е направен на истиот начин на кој се опиша и хибридното решение. Како изведени компоненти во моделот се појавуваат **Average job1 data throughput** и **Average job2 data throughput,** како променливи кои ја прикажуваат средната вредност на количествата податоци пренесени до заштитното складиште на системот (RSV), променливата **Average recovery time per MB** која го прикажува потребното време за оправување на 1MB количество податоци поставено во заштитното складиште на системот и **Total service cost/month** како изведена променлива која ги прикажува трошоците за користење на складишниот сервис поставен во облак.

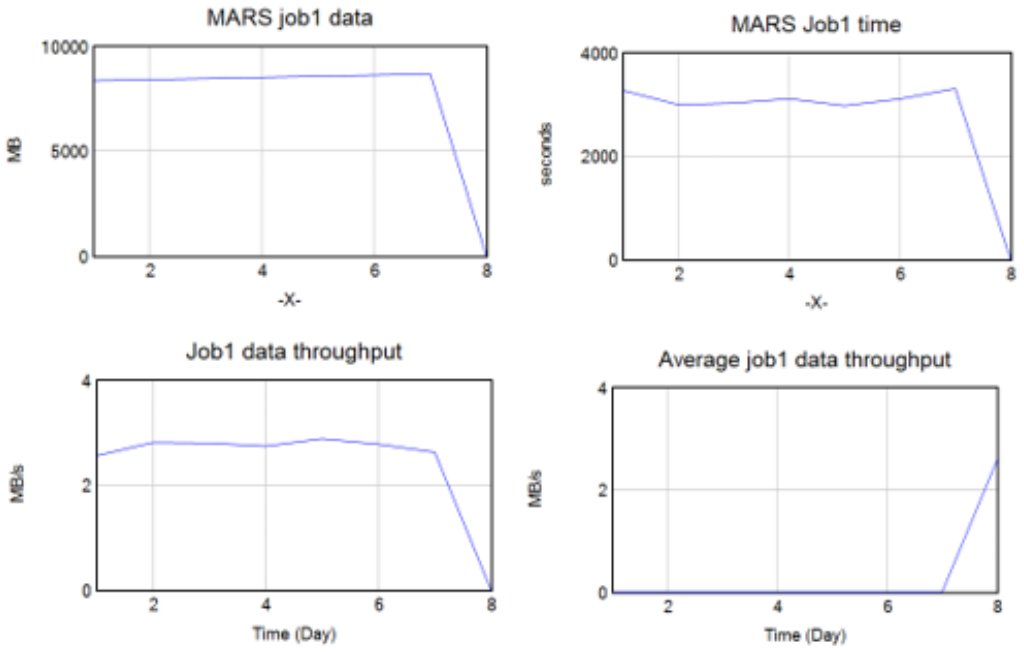
Временскиот период во кој се изведуваат процедурите за правење на копии и враќање на податоците од нив, опфаќа 8 временски точки, од кои 7 се наменети за изведување на политиката за правење на сигурносни копии, а последната временска точка е наменета за прикажување на промената на количеството податоци кои се поставени во складиштето по исполнување на циклусот од 7 дена, согласно вредностите дадени во Табела 1. Состојбите на вредностите на променливите во основниот модел и нивните промени во поставената временска рамка се прикажанив во Табела 4, каде во посебен дел се прикажани и конечните вредностите на изведените компоненти по завршена симулација со зададените влезни параметри. На Слика 8 е даден графички приказ на состојбите на влезните компоненти во моделот поврзани со процесот MARS job1, а на

Слика 9 е даден графички приказ на состојбите на компонентите поврзани со процесот MARS job2.

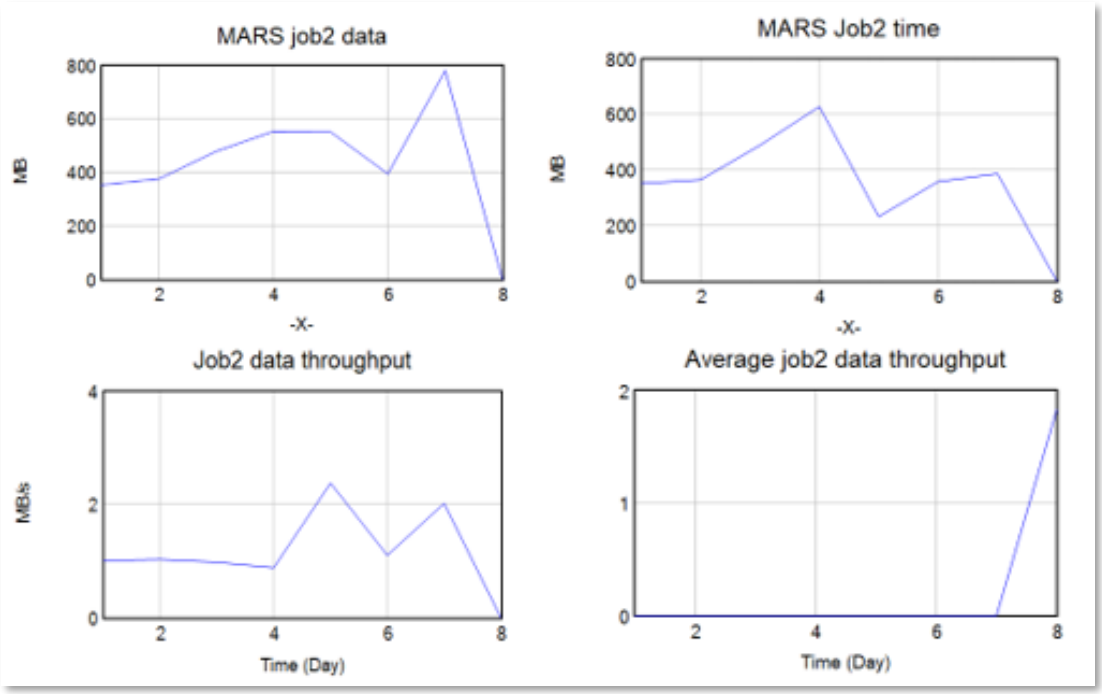
Variable	Value							
	1	2	3	4	5	6	7	8
Data backup process								
MARS job1 data (MB)	8362	8409	8463	8516	8569	8622	8678	
MARS Job1 time (sec)	3270	2993	3025	3110	2976	3105	3307	
Job1 data throughput (MB/s)	2.55719	2.80956	2.79769	2.73826	2.87937	2.77681	2.62413	
MARS job2 data (MB)	353	375	478	553	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

Табела 4 *Вредносни состојби на променливите во основниот модел*

Добиените вредности од симулацијата кои се однесуваат на изведените компоненти прикажани во Табела 4, се основа за спроведување на евалуација на перформабилноста на системот при манипулирање со екстремни вредности на податочните компоненти, кои како такви имаат директно влијание во менувањето на перформансите на системот.



Слика 8 *Графички приказ на вредностите на компонентите поврзани со MARS job1*

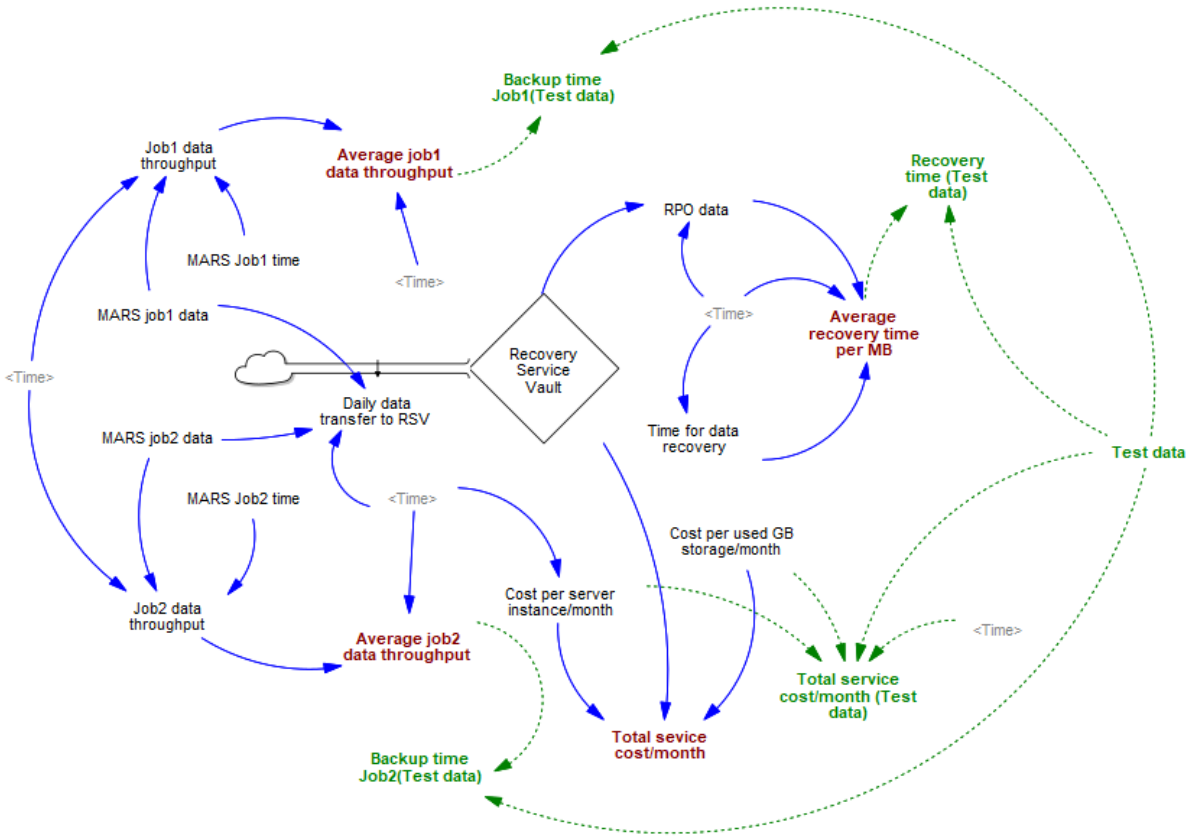


Слика 9 *Графички приказ на вредностите на компонентите поврзани со MARS job2*

За таа цел кон моделот кој е претставен како основен и од кој се искористени изведените компоненти, се додадени пет нови компоненти од кои:

- две компоненти **(Backup time Job1(Test data)** и **Backup time Job2(Test data))** за калкулирање на времињата за создавање на копии со двата процеси,
- една компонента која се однесува на процесот за оправување на податоците **(Recovery time (Test data))**,
- една компонента заедничка за сите, која ја носи вредноста на количината податоци која ја има серверски систем во организацијата (Test data = 531 GB), и
- една компонента **(Total service cost/month (Test data))** за калкулирање на трошоците за користење на сервисот со новата количина на податоци.

Приказот на проширениот модел со новите компоненти е даден на Слика 10, а резултатите од изведување на симулацијата се прикажани во Табела 5.



Слика 10 *Модел на систем во облак со дополнителни компоненти*

Variable	Value
Derived variables (basic model)	
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 (extended model)	
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

Табела 5 *Резултати од симулација на проширен модел за систем во облак*

Поради високите вредности на состојбите кај временските компоненти, приказот за овие вредности е даден во часови, а вредноста на податоците во MB.

3.1.3 Компаративна анализа

За добивање на целовита слика за перформабилноста на двата системи, во дисертацијата е направена компаративна анализа на добиените резултати од изведените

симулации на прикажаните модели. Со примена на вредностите добиени од системите за заштита на податоците, во компаративен преглед поделени по операции во три табели, ставени се компонентите кои во симулациите се означени како изведени. Во првата табела (Табела 6) е направен компаративен преглед на количествата податочен трансфер кај двата системи при процесот на создавање на сигурносна копија од податоците.

Систем	ХИБРИДЕН (*DP 4400*)	ВО ОБЛАК (*Azure Recovery service*)	
Компонента	Average daily data throughput (to AVS)	Average job1 data throughput	Average job2 data throughput
Вредност (MB/s)	**54.2224**	**2.57731**	**1.83045**

Табела 6 *Вредности на податочен трансфер при создавање на сигурносна копија*

Според дадениот преглед, евидентно е дека хибридниот систем има многукратно поголем податочен трансфер во единица време помеѓу Avamar агентот и AVS при изведување на процесот за создавање на сигурносна копија. Ова се должи пред се на комуникациската врска помеѓу двете крајни точки на процесот, каде во хибридниот систем врската е преку локалната мрежа, а кај системот во облак почетната точка се наоѓа во податочниот центар (MARS агентот), поминува преку интернет операторот (ISP) и завршува во сервисот поставен во облак. Ваквите промени на податочните трансфери неминовно носат деградација на перформансите, а резултатот е сумарен пропусен опсег со мали вредности, кои директно влијаат на времетраењето на процесот со кој се создаваат копиите. Компаративниот приказ на резултатите од симулација на процесите за оправување на податоците со резултантните компоненти кои се изведени од вредности добиени од овие процеси во двата системи, се прикажани во Табела 7.

Систем	ХИБРИДЕН (*DP 4400*)		ВО ОБЛАК (*Azure Recovery service*)
Компонента	Restore time per MB (LOCAL)	Restore time per MB (ARCHIVE)	Average recovery time per MB
Вредност (sec)	**0.02096**	**0.25773**	**5.57246**

Табела 7 *Потребно време во процес на оправување за 1MB податоци*

Од прикажаните резултати во табелата се забележува дека кај хибридниот систем, процесот на оправување на податоците од локалното складиште на уредот има многу пократко време од процесот кој побарува податоци поставени во складиштето во облак.

Користењето на складишта во облак од страна на опишаните системи за заштита и оправување на податоци, носи со себе и трошоци кои се резултат на користењето на

услугата во облак. Во Табела 8 е даден приказ на овие трошоци и параметрите по кои истите се направени.

Систем	ХИБРИДЕН (*DP 4400*)	ВО ОБЛАК (*Azure Recovery service*)
Cost per server instance/month	/	10
Cost per used GB storage/month	0.02	0.0448
Cost per ingress/egress transactions ($/10 K oper.)	0.54	/
Cost per listing contents ($/10 K oper.)	0.5	/
TOTAL COST for TEST DATA ($/month)	11.66	43.79

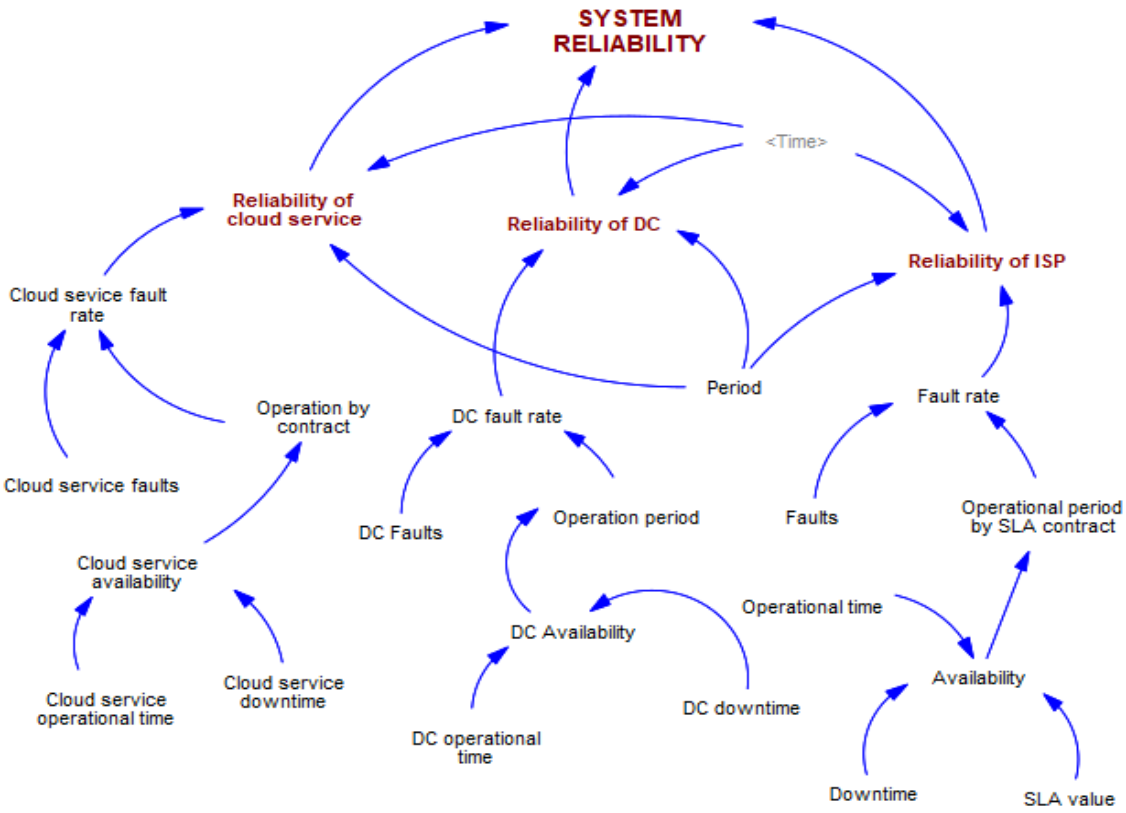
Табела 8 *Месечни трошоци за користење на сервис во облак за двата системи*

Последната ставка на табелата ги прикажува трошоците при користење на складишен простор еднаков на количеството податоци (531 GB) кое беше користено при симулациите за двата системи во случаите на нивните проширени модели.

3.1.4 Анализа на надежност

Според поставеноста на компонентите во системот кој го прикажува концептот за заштита на податоци од испади и катастрофи, тој во себе вклучува три компоненти: податочниот центар (DC), сервисот во облак (Azure) и врската кон глобалната мрежа. Со вака поставен концепт на системот, тој може да се прикаже како сериска врска помеѓу неговите компоненти каде испадот на било која компонента во системот (не оперативна бинарна состојба на компонентата, за која ќе важи R=0), ќе значи испад и на целиот систем. Вака поставеното размислување за оперативноста на целиот систем е основа за анализа на неговата надежност. При градењето на модел за калкулирање и проценка на надежноста на системот, во нашиот случај подразбира поставување на повеќе променливи во него кои ќе ги претставуваат условите од кои зависи надежноста на секоја од неговите компоненти. Почетните услови за поставување на концептот на моделот ги опфаќа: периодот во кој ќе се користи податочниот центар (предвидени 7 години или 61320 часа), периодот во кој се изведува анализата на системот (15 дена или 360 часа), оперативното време на операторот на врската кон глобалната мрежа (базирано на договорот за користење од 24 месеци или 17520 часа) и нивото на Service Level Agrement (SLA) од 99.95%. Моделот за анализа на надежност на концептите за податочна заштита со вака поставени почетни услови е прикажан на Слика 11, а резултатите од изведената

симулација за надежност на секоја од компонентите и системот како целина, се дадени во Табела 9.



Слика 11 *Модел за надежност на систем од три компоненти*

Назив на компонента	Вредност
Reliability of cloud service	0.993952
Reliability of DC	0.993952
Reliability of ISP	0.978981
SYSTEM RELIABILITY	0.967174

Табела 9 *Надежност за компонентите и системот за даден период*

Од приказот на резултатите, може да се заклучи дека и покрај високите вредности за надежност на сервисот во облак и податочниот центар (надежноста за нив во почетните услови е поставена на R=1), пониската вредност за надежност кај операторот има негативно влијание на надежноста на целиот систем. Тоа се должи на сериската врска на овие компоненти во извршување на процесите кои го користат сервисот во облак. Во Disaster Recovery Journal (DRJ)[1], се наведува дека секое сценарио или концепт на вакво

[1] HTTPS://DRJ.COM/JOURNAL_MAIN/BACKUP-AND-DISASTER-RECOVERY-SERVICES-ONLY-AS-RELIABLE-AS-YOUR-NETWORK-CONNECTION

решение е надежно онолку колку што е надежна неговата врска кон глобалната мрежа. Според тоа, во концепти на системи кои се базирани на сервис во облак или сервис од било каков вид кој користи врска со глобалната мрежа, при дизајнирање на ваквите решенија, задолжително е потребно внимателна проценка на вредностите во SLA документите, бидејќи мали отстапки во нив придонесуваат за забележителни промени во карактеристиките кај останатите компоненти, а со тоа и на целото поставено решение.

3.1.5 Заклучни согледувања

Во современото деловно работење и неговата забрзана дигитална трансформација, се истакна важноста на податоците и системите во кои тие се наоѓаат, поставувајќи ги податоците на централно место во информацискатa размена. Ваквата зависност на деловните процеси, наметнува развој и поставување на решенија за нивна заштита, со цел одржување на нивниот деловен континуитет. Постојат повеќе решенија на системи со ваква намена, секој со свои предности и недостатоци во начинот на кој ја остваруваат заштитата на деловниот континуитет. Дел од нив се целосно насочени кон сигурно и безбедно чување на податоците (backup data), дел се наменети за нивна заштита со чување на активните податоци во две и повеќе локации, поврзани со процеси за постојана или повремена синхронизација помеѓу нив (replication), а дел се наменети за одржување на два или повеќе податочни центри на организациите, за одржување на непрекинат деловен континуитет. Главната придобивка од истражувањето спроведено во дисертацијата се однесува на утврдување на параметрите кои имаат клучна улога во градењето на правилен пристап кон избор на решение или решенија кои во целост ќе ги задоволат барањата и потребите поставени во BIA, со цел успешно одржување на деловниот континуитет на организациите чие работење е целосно базирано на информациски системи. Врз основа на ова, заклучните согледувања во дисертацијата се поделени на заклучоци од технички аспект, од аспект на карактеристики и перформанси и финансиски аспект, за во завршниот дел да се дадат согледувања и препораки за можни идни истражувања за унапредување на пристапот кон добивање повисоки вредности за перформабилноста и надежноста на системите за податочна заштита. Имајќи предвид дека количествата податоци имаат директно влијание на временските компоненти на решенијата за заштита, како идни насоки за истражување треба да бидат механизмите кои ќе придонесат за поголемо редуцирање на податоците кои ќе бидат разменувани помеѓу системите во целиот процес на заштита. Од технички аспект, како и од аспект на перформансите на решенијата за заштита, според резултатите добиени од моделите развиени за двата разгледувани системи, користењето на решение кое ќе биде поставено

локално со распределување на податоците во облак како ниво од целокупното складиште на уредот (single data namespace), обезбедува доволна заштита во случај на испад и ги задоволува потребите за брзо враќање во оперативна и функционална состојба на информатичките и информациските системи кои се користат за секојдневно работење. Во однос на трошоците за користење на сервисот во облак, треба да се има предвид кога се користат ваквите сервиси за чување на поголеми количини податоци, дека коефициентот кој најмногу ја зголемува вредноста на компонентата Total service cost/month е токму делот кој се однесува на наплатата за зафаќање на складишен простор, односно количината на податоци која ќе биде сместена во складиштето.

4 ОРГАНИЗАЦИЈА НА ДОКТОРСКАТА ДИСЕРТАЦИЈА

Поради високата стапка на неуспех во процесите за оправување на информациските системи на копманиите при посериозен прекин, во докторската дисертација се обработува оправувањето од катастрофи како составен дел од деловниот континуитет и во седум поглавја, се прави анализа на перформибилноста и надежноста на системите кои се обработени и нивната практична имплементација во реални сценарија. Како вовед во темата, во првите три поглавја, направен е преглед на теоретските основи на кои се темели истражувањето, поврзано со податочните центри, информациските системи и концептите за деловен континуитет во организациите чие работење е поставено на дигитални основи.

Во **првата глава** на дисертацијата, во вкупно пет под глави, се прави кус осврт кон она што ќе се обработува во останатиот дел од трудот. Притоа, се прави осврт кон предметот на истражувањето, се наведуваат целите на истражувањето, се прави осврт кон применетата методологија, за на крајот да се направи краток преглед на резултати и придобивки од спроведеното истражување. Во рамки на оваа глава, даден е преглед на претходно спроведени истражувања за решенија кои се поврзани со сервиси во облак и решенија кои го обработуваат процесот на оправување од катастрофи како концепт.

Втората глава ги обработува основите на кои се темели дисертацијата, а тоа се податочните центри (Data Centers-DC) и информациските системи поставени во нив. Притоа се прави дефинирање и поделба на податочните центри според начинот на изведба и нивните карактеристики како важни параметри во одржување на деловниот континуитет, а во продолжение се прави и осврт на неколку клучни аспекти поврзани со нивната работа, со посебен акцент на обработка на информациските системи. Информациските системи ќе бидат обработени преку нивно дефинирање како системи, дефинирање на термините информација, податок и систем како основни за нивното

функционирање, за во продолжение да се направи преглед и класификација според нивната употреба, како важен податок при градењето на плановите за деловен континуитет.

Првиот дел од **третата глава** го обработува деловниот континуитет како концепт, накратко ги опишува методите за обезбедување на деловен континуитет постигнат со широко применети конвенционални методи како вовед кон современите системи за планирање на одржлив деловен континуитет, заснован на клучните параметри во процесот на планирање, но и на заклучоците добиени по спроведување на анализата за влијанието на прекинот во целокупното работење (*Business Impact Analyses-BIA*). Во вториот дел од главата се прави осврт кон процесот на оправување од испади и катастрофи преку негов опис и дефинирање, а во продолжението се утврдуваат и детално се опишуваат клучните параметри по кои се вреднува процесот на оправување. Во прилог на правилно поставување на основните аспекти на процесот за оправување, се разгледуваат и специфицираат побарувањата на процесот, за негово правилно планирање и спроведување.

Согласно темата, во **четвртата глава** се прави опис на практично имплементирани решенија за оправување од испади и катастрофи преку дефинирање на потребите за реализација, конструктивните елементи и нивните карактеристики применети во решенијата. Во продолжение се разгледуваат две сценарија на системи за оправување од кои едниот е хибридно решение базирано на систем поставен во податочниот центар на место, со ниво на обезбедување поставено во облак како крајна точка (*endpoint*), а другиот систем е сценарио целосно базирано на облак.

Во рамки на **петата глава** се определуваат и дефинираат клучните параметри по кои се прави анализата и оценката на предложените системи. Во продолжение се прави нивно поврзување во функционална спрега преку примена на *System Dynamics* пристап за секој од разгледуваните системи посебно, за на крајот да се направи нивна компаративна анализа. Изведувањето на симулации од типот „ што ако “за тестирање на одредени политики на таков модел, има голем придонес во разбирањето како системот се менува со текот на времето, а со тоа и на одредувањето на параметрите кои ќе бидат поставени како целни во плановите за оправување и одржување деловен континуитет во работењето на организациите. Во текот на сумирање на добиените резултати и нивното графичко прикажување, паралелно се разгледуваат и перформансите на компонентите кои учествуваат во процесот за заштита на податоците. Ваквото сумирање има за цел добивање јасна претстава за перформансите на системите во процесите за обезбедување на податочните центри.

Шестата глава ги дава заклучните согледувања базирани на поставените системи за оправување од катастрофи и анализата на нивните перформанси. Притоа се истакнуваат клучните предности и недостатоци на секое од нив во обработените сценарија на примена. Во рамки на оваа глава се резимирани и определени резултати и заклучоци од направените истражувања. Во завршниот дел се даваат насоки за понатамошна работа, со цел добивање на подобри перформанси на користените решенија.

Во **седмата глава** е даден преглед на целокупната литература која е користена при истражувањето и пишувањето на трудот. Во посебен оддел од ова поглавје наведени се интернет изворите кои беа користени како нужен информациски извор за современите достигнувања во областите кои беа опфатени со истражувањето.

5 БИБЛИОГРАФИЈА

[1] A. Bokhary, "Cloud Service Reliability and Usability Measurement", Computer Science and Engineering Theses and Dissertations, Southern Methodist University, 2018

[2] A. Marcham,"Understanding Infrastructure Edge Computing: Concepts, Technologies and Considerations", First Edition, John Wiley & Sons Ltd, New Jersey, 2021.

[3] 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

[4] A.A. Tamimi, R. Dawood, L. Sadaqa, "Disaster Recovery Techniques in Cloud Computing", IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019, Amman, Jordan.

[5] A.Hiles, "The Definitive Handbook of Business Continuity Management Second Edition", John Wiley & Sons, Chichester, West Sussex, England, 2007

[6] A.Lenk, "Cloud Standby Deployment:A Model-Driven Deployment Method for Disaster Recovery in the Cloud", 8th International Conference on Cloud Computing, 2015, New York City

[7] A.Mishra, V.Sharma, A.Pandey, "Reliability of Cloud Computing Services", IOSR Journal of Engineering, Volume:04, Issue:01, pp.51-60, 2014

[8] A.Mishra, V.Sharma, A.Pandey, "Reliability, Security and Privacy of Data Storage in Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 5, No.3, 2014

[9] B. Chakraborty, Y. Chowdhury, "Introducing Disaster Recovery with Microsoft Azure: Understanding Services and Tools for Implementing a Recovery Solution", Apress, 2020

[10] C. Bertrand, M. Keane, "Cloud-ready Data Protection with Dell EMC", ESG White Paper, The Enterprise Strategy Group, 2018

[11] C. Garnier, M. Aggar, M. Banks, J. Dietrich, B. Shatten, M. Stutz, and E. Tong-Viet, "Data center life cycle assessment guidelines," The Green Grid, White Paper-45, 2012.

[12] C. M. Pearson and J.A. Clair, "Reframing crisis management", Pearson,1998

[13] D.M.Vistro, A.U.Rehman,S.Mehmood,M.Idrees, A.Munawar, "A LITERATURE REVIEW ON SECURITY ISSUES IN CLOUD COMPUTING: OPPORTUNITIES AND CHALLENGES", JOURNAL OF CRITICAL REVIEWS, Volume:7,Issue:10, 2020

[14] D.Sutton, "Business Continuity in a Cyber World: Surviving Cyberattacks", Business Expert Press, New York, 2018

[15] Data Protection and Management", Participant guide, Dell Technologies Inc, USA, 2021

[16] E.Bauer, R. Adams, "Reliability and availability of cloud computing", IEEE Press, John Wiley & Sons, New Jersey, 2012

[17] E.Dubrova, "Fault-Tolerant Design", KTH Royal Institute of Technology, Sweden, Springer Science+Business Media, 2013, New York

[18] E.J. McClusky, S. Mitra, "Fault Tolerance" in Computer Science Handbook 2ed. ed. A.B. Tucker. CRC Press, (2004)

[19] H. Geng, "Data center handbook: plan, design, build, and operations of a smart data center", John Wiley & Sons, 2021

[20] H.B.Rebah, H.B.Sta, "Disaster Recovery as a Service: A Disaster Recovery Plan in the Cloud for SMEs", Global Summit on Computer & Information Technology, 2016, Sousse, Tunisia

[21] H.C.Lucas, Information Systems Concepts for Management, McGraw-Hill, New York, 1978, p.5

[22] H.E. Miller, K.J. Engemann, "Using reliability and simulation models in business continuity planning",International Journal of Technology, Policy and Management, Vol. 5, No. 1, 2014, pp.43-56

[23] I.Gertsbakh, "Reliability Theory", Springer-Verlag Berlin Heidelberg, NewYork, 2005

[24] J.Chan, M.Reith, "Cyber Concerns With Cloud Computing", Proceedings of the 21st European Conference on Cyber Warfare and Security, Reading, Chester, United Kingdom, 2022

[25] J.Li , P.Li, R.J.Stones, G.Wang, Z.Li, X.Liu, "Reliability Equations for Cloud Storage Systems with Proactive Fault Tolerance", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 15, 2018

[26] J.Mendonça, R.Lima, E.Andradey, J.Araujoy, D.S.Kim, "Multiple-criteria Evaluation of Disaster Recovery Strategies Based on Stochastic Models", 16th International Conference on the Design of Reliable Communication Networks (DRCN), IEEE, 2020

[27] J.Mendonca, R.Lima, E.Queiroz, E.Andrade, D.S.Kim, "Evaluation of a Backup-as-a-Service Environment for Disaster Recovery", IEEE Symposium on Computers and Communications (ISCC), 2019, Barcelona, Spain

[28] J.Mendonca, R.Lima, R.Matos, J.Ferreira, E.Andrade, "Availability Analysis of a Disaster Recovery Solution Through Stochastic Models and fault enjection experiments",32nd International Conference on Advanced Information Networking and Applications, IEEE, 2018

[29] Jaroslav Menčík, "Concise Reliability for Engineers", Intechopen, 2016

[30] Joseph M. Firestone, Enterprise Information Portals and Knowledge Management, Elsevier Science, Burlington, 2003, p.4

[31] 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, 2012

[32] L.Tomás, P.Kokkinos, V.Anagnostopoulos, O.Feder, D.Kyriazis, K.Meth, E.Varvarigos, T.Varvarigou, "Disaster Recovery Layer for Distributed OpenStack Deployments", IEEE Transactions on Cloud Computing, Volume: 8, 2017

[33] Le secours du SI dans le Cloud, Faut-il faire le grand saut du DRaaS ?, Livre blanc, Lexsi, 2014.

[34] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges", Information Sciences, Vol.305, 2015, pp. 357-383

[35] M. Whitman, H. Mattord, "Principles of Incident Response & Disaster Recovery", 3rd Edition, Cengage Learning, 2021

[36] M.A.Khoshkholghi, A.Abdullah, R.Latip, S.Subramaniam, M.Othman, "Disaster Recovery in Cloud Computing: A Survey", Computer and Information Science, Vol. 7, No. 4, 2014

[37] M.Ali, K.Bilal, S.U.Khan, B.Veeravalli, K.Li, A.Y.Zomaya, "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security", IEEE Transactions on Cloud Computing, Volume: 6, Issue: 2, 2018

[38] M.M. Alshammari, A.A. Alwan, A. Nordin, I.F. Al-Shaikhli, "Disaster Recovery in Single-Cloud and Multi-Cloud Environments: Issues and Challenges", (ICETAS), 2017, Salmabad, Bahrain

[39] M.S. Fernando, “IT Disaster Recovery System to Ensure the Business Continuity of an Organization,” National Information Technology Conference (NITC), 13-15 September,2017, Colombo, Sri Lanka

[40] M.Wallace, L.Webber, "THE DISASTER RECOVERY HANDBOOK SECOND EDITION", American Management Association, USA, 2011

[41] N.Dhanujati, A.S.Girsang, "Data Center-Disaster Recovery Center (DC-DRC) For High Availability IT Service", International Conference on Information Management and Technology (ICIMTech), 2018, Jakarta

[42] O.H.Alhazmi, Y.K.Malaiya, "Assessing Disaster Recovery Alternatives: On-site, Colocation or Cloud", 23rd International Symposium on Software Reliability Engineering Workshops, 2012, Dallas

[43] O.V.G. Swathika, K. Karthikeyan S. Padmanaban, "Smart Buildings Digitalization: Case Studies on Data Centers and Automation", CRC Press, 2022, Abingdon

[44] P. Da, P.M. Khilar,"Virtualization and fault tolerance for cloud computing", Proceedings of 2013 IEEE Conference on Information and Communication Technologies, 2013

[45] P.J.Mitrevski, I.S.Hristoski, "Behavioral-based performability modeling and evaluation of e-commerce systems", Electronic Commerce Research and Applications (13), p.320-340, Elsevier, 2014

[46] P.A.Longley, M.F.Goodchild, Geographical Information Systems and Science, John Wiley&Sons, West Sussex, 2005, p.30

[47] R.Asciento, A.Lawrence, "Uptime Institute global data center survey 2020", Uptime Institute, Seattle, USA, 2020

[48] R.H. Bowman Jr., "Business Continuity Planning for Data Centers and Systems", John Wiley & Sons, New Jersey, 2008.

[49] S. Kambhampaty, "Infrastructure Architecture Essentials for Data Center and Cloud", Independently published, 2022

[50] S. Shahzadi, G. Ubakanma, M. Iqbal, T. Dagiuklas, "Autonomous, Seamless and Resilience Carrier Cloud Brokerage Solution for Business Contingencies During Disaster Recovery", IEEE 20th International Conference on High Performance Computing and Communications, 2018, Exeter, UK.

[51] S. Snedaker, C. Rima, "Business Continuity and Disaster Recovery Planning for IT Professionals", Second Edition, Elsevier, 2014

[52] S.A.M. Kasim, I. Mohamed, "Level of Readiness in IT Disaster Recovery Plan", Cyber Resilience Conference, 2018, Putrajaya, Malaysia

[53] S.Al-Kiswany, M.Ripeanu,"A software-defined storage for workflow applications", IEEEInternational Conference on Cluster Computing, IEEE International Conference (CLUSTER), Taipei, Taiwan, p. 350–353, 2016

[54] S.Anthoniraj, Dr. S.Saraswathi, M.Anandraj, "Disaster recovery planning using fault tolerant mechanism in virtualization environment", Fourth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom2012), 2012, Bangalore, India.

[55] S.C. Joshi and K.M. Sivalingam, "Fault tolerance mechanisms for virtual data center architectures", Springer Science+Business Media, 2014, New York

[56] S.D.Lowe et al.,"Building a Modern Data Center Principles and Strategies of Design", ActualTech Media, Bluffton, 2016

[57] S.Wei, H.Yang, J.Song, F.Mikayilov, Z.Xu, "System Dynamics Simulation Model for Assessing Socio-Economic Impacts of Different Levels of Environmental Flow Allocation in the Weihe River Basin",European Journal of Operational Research, Volume 221, pp.248–262, 2012

[58] Scalable Data Protection for Microsoft Windows Server Software-Defined Solutions", White Paper H17894, Dell Technologies, USA, 2019

[59] T. Wood, E. Cecchet, K. Ramakrishnan, P. Shenoy, J. Van Der Merwe, A. Venkataramani, "Disaster recovery as a cloud service: Economic benefits & deployment challenges", 2nd USENIX Workshop on Hot Topics in Cloud Computing, 2010, Boston.

[60] T.Tsubaki, R.Ishibashi, T.Kuwahara, Y.Okazaki, "Effective disaster recovery for edge computing against large-scale natural disasters", IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), 2020, Las Vegas, NV, USA

[61] U. C. Kozat,G. Liang,"Building Reliable Storage Clouds: Models,Fundamental Tradeoffs, and Solutions",Now Foundations and Trends,2015

[62] V. Kumar, R. Vidhyalakshmi, "Reliability Aspect of Cloud Computing Environment", Springer Nature Singapore Pte, Singapore, 2018

[63] V.Sivaraj,A.Kangaiammal, A.Kashyap, "Enhancing Fault Tolerance using Load Allocation Technique during virtualization in cloud computing",7th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2021

[64] W. T. Coombs, "Ongoing crisis communications: planning, managing and responding", 5th ed, Sage, 2019

[65] W.P.Turner, J.H.Seader, K.G.Brill, "Industry standard tier classifications define site infrastructure performance", White Paper, The Uptime Institute, 2005

[66] Weill, P., Broadbent, M., "Leveraging the new infrastructure", Harvard Business School Press, Boston, 1998

[67] Z.Liu, G.Fan, H.Yu, L.Chen, "An Approach to Modeling and Analyzing Reliability for Microservice-Oriented Cloud Applications", Hindawi Wireless Communications and Mobile Computing, Volume 2021, Article ID 5750646, 2021