Sistema de còpies de seguretat per a servidors domèstics

Xavier Lapuente Salinas

Resum—En aquest projecte s'ha desenvolupat un sistema que permet fer còpies de seguretat xifrades entre servidors per a ús domèstic. En aquest article s'explica la metodologia de desenvolupament que s'ha seguit durant el projecte, així com les funcionalitats del sistema desenvolupades que han permès aconseguir els objectius establerts. El motiu per el que s'ha implementat aquesta solució és perquè actualment no hi ha un sistema que permeti als usuaris realitzar còpies de seguretat en remot entre servidors domèstics. Les plataformes que permeten realitzar còpies de seguretat al núvol són tecnologies de pagament que tenen un cost en funció de la quantitat d'informació que els usuaris hi emmagatzemen. Els resultats obtinguts de la implementació del sistema ens porten a concloure que és totalment viable el desplegament del projecte, tot i que encara es pot extendre amb noves funcionalitats que el deixerien llest per ser posat en producció. En aquest article es detallen les tasques de desenvolupament realitzades durant el projecte i es mostren les proves que s'han realitzat. Finalment, s'analitzen els resultats obtinguts d'aquestes proves i s'extreuen unes conclusions.

Paraules clau—Còpia de seguretat, servidor domèstic, Local Area Network (LAN), xifrat, router, IP, sistema de fitxers, interfície d'usuari, ample de banda.

Abstract—In this project we have developed a system that allows the users to do encrypted backups of the information stored in a home server in an other private home server. In this article we explain the methodology used during the development of the project and also the different functionalities developed to achieve the planned objectives. The reason why this project has been developed is because nowadays there is not a system that allows people to backup their home servers data in an other remote home server. The current technologies that are available to do backups online are private services that have a cost depending on the amount of data needed by the user. The results obtained in the project lead us to conclude that is completely feasible the development of this project. However, in the current state, there are some functionalities that are still pending due to lack of time. In this article we present the development tasks done during the project and there are shown the tests executed. Finally, the results obtained in the tests are analyzed and we extract some concusions.

Index Terms—backup, home server, Local Area Network (LAN), encryption, router, IP, file system, user interface, bandwidth

1 INTRODUCCIÓ

ACTUALMENT les persones tenen molta informació personal emmagatzemada en dispositius electrònics. Quan hi ha un problema tècnic amb els dispositius on hi ha la informació emmagatzemada i no és possible recuperar-la és quan es valora la importància de tenir còpies de seguretat de la informació que no es vol perdre. Les tecnologies que actualment permeten realitzar còpies de seguretat en local són, entre altres, els servidors domèstics. Un servidor domèstic s'utilitza per guardar còpies de seguretat en una LAN de una família o una petita empresa. Els dispositius que formen part de la LAN es connecten al servidor domèstic i realitzen les còpies de seguretat en aquest servidor. En la Figura 1 es presenta un esquema genèric de una LAN actual. Hi ha un router connectat a Internet i els diferents dispositius connectats a la LAN que crea el router. El servidor domèstic permet compartir fitxers i realitzar còpies de seguretat als dispositius de la LAN.

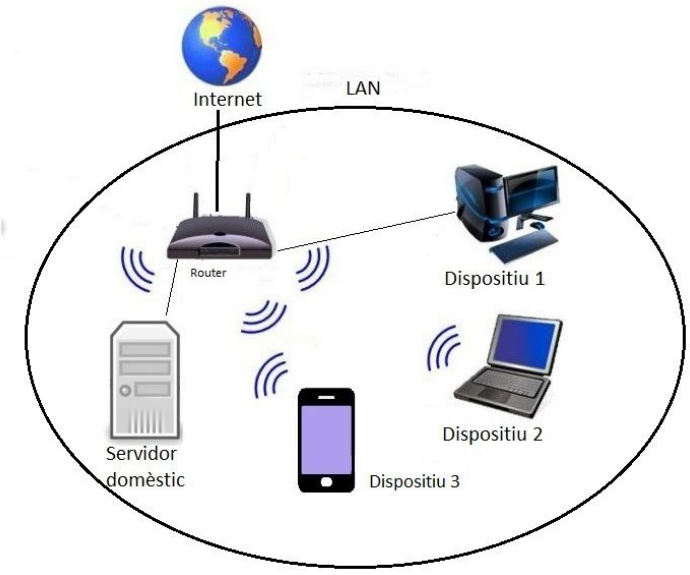

Figura 1. Esquema de una LAN genèrica on s'utilitzen servidors domèstics.

- *E-mail de contacte: xavier.lapuente@e-campus.uab.cat*
- *Menció realitzada: Tecnologies de la Informació*
- *Treball tutoritzat per: Sergi Robles Martínez (dEIC)*
- *Curs 2016/17*

La solució proposada en aquest article es basa en un sistema que permet realitzar còpies de seguretat en remot i xifrades entre servidors domèstics. A continuació es proposa una situació genèrica on es podria aplicar la solució proposada en el projecte. Suposem que l'usuari 1 té un servidor domèstic a casa seva, i l'usuari 2 també té un altre servidor domèstic. L'objectiu del nostre projecte és que l'usuari 1 pugui fer còpies de seguretat del seu servidor al servidor de l'usuari 2 i viceversa sense que hi hagi un cost econòmic per part dels usuaris. L'únic cost que han d'assumir els usuaris del sistema que proposem són els costos dels dispositius hardware del sistema.

En el sistema proposat cada servidor domèstic tindrà dues particions (poden ser físiques o lògiques). En una partició s'emmagatzemen les còpies de seguretat dels usuaris de la LAN on està el servidor. En l'altre partició del sistema s'emmagatzemen una còpia de tot el sistema de fitxers del servidor remot on fem les còpies de seguretat.

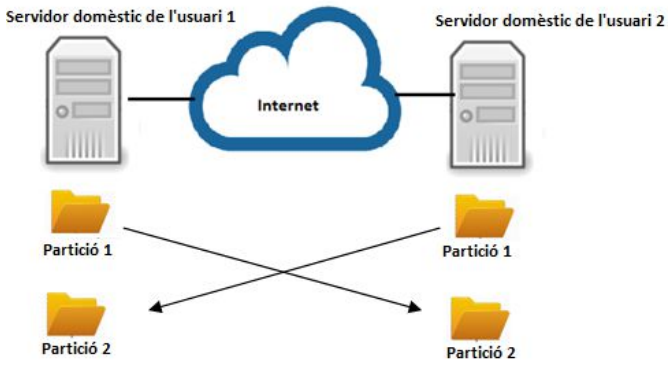

Figura 2. Esquema de la solució proposada en el projecte. Els servidors domèstics utilitzen la partició 2 de altres servidors domèstics per realitzar còpies de seguretat en remot.

D'aquesta manera, en el servidor de l'usuari 1 hi ha emmagatzemades les còpies de seguretat dels dos servidors domèstics, i en el servidor de l'usuari 2 també hi ha emmagatzemades les còpies dels dos servidors.

La nostre solució permet realitzar de manera fàcil i intuïtiva pels usuaris la gestió d'aquestes còpies de seguretat. També permet els procediments de recuperació d'informació del servidor remot al servidor local. Per qüestions de privacitat i per aspectes legals, les còpies de seguretat realitzades en remot es xifraran utilitzant una clau que especificarà l'usuari propietari del servidor local. Aquest xifrat de les dades es farà abans de enviar la informació al servidor remot de manera que quan les dades del propietari siguin enviades al servidor estaran xifrades.

En aquesta secció s'ha exposat la introducció del projecte. En les següents seccions s'expliquen els objectius del projecte, l'estat de l'art, la metodologia utilitzada, el desenvolupament del projecte i, finalment, els resultats obtinguts.

2 OBJECTIUS

En aquesta secció es presenten els objectius del projecte. També s'exposen de manera ordenada els subobjectius prioritzats.

L'objectiu principal d'aquest projecte és desenvolupar un sistema de seguretat per a servidors domèstics. El servidor domèstic emmagatzema qualsevol informació que els usuaris del sistema volen tenir en còpia de seguretat o bé que volen compartir entre ens usuaris de la LAN. Tota la informació que s'emmagatzema en aquest servidor serà enviada al servidor remot en el moment que es realitzen les còpies de seguretat. Per aconseguir aquest objectiu, s'han planificat els següents subobjectius de manera prioritària:

1- Analitzar les tecnologies disponibles que podem utilitzar per implementar la nostre solució. Aquest subobjectiu es basa en estudiar les tecnologies que actualment s'utilitzen en sistemes com el que volem implementar per determinar quines es poden integrar i quines són les que millor s'adapten a la solució que es vol desenvolupar.

2- Realitzar l'anàlisi de requisits del sistema a desenvolupar. Aquest subobjectiu ens permet tenir documentats els requisits del sistema que es vol implementar i una descripció del comportament d'aquest sistema.

3- Dissenyar el nostre sistema. Aquest subobjectiu consisteix en realitzar un disseny de la solució que es vol desenvolupar per tenir clar que es vol fer en el procés d'implementació del sistema.

4- Implementar el sistema. En aquest subobjectiu s'implementa la solució prèviament dissenyada, tenint en compte els subobjectius prèviament plantejats.

En aquesta secció s'ha exposat l'objectiu principal del projecte i, de manera prioritzada, els subobjectius que es plantegen per aconseguir l'objectiu principal.

3 ESTAT DE L'ART

Actualment hi ha diverses maneres de realitzar còpies de seguretat de la informació personal que tenim en els nostres dispositius. Les maneres més comuns de fer-ho són mitjançant dispositius externs com disc durs on realitzem còpies de seguretat manualment cada cert període de temps de la informació que ens interessa. El problema és que en aquesta situació en cas que el dispositiu on esta emmagatzemada la informació deixi de funcionar, es perd tota la informació de còpies de seguretat.

També és possible contractar serveis de emmagatzematge remot on és possible realitzar les còpies de seguretat. Aquests serveis tenen un cost mensual en funció de la quantitat d'espai que s'utilitza [1]-[3].

La opció que més s'aproxima al nostre projecte és la dels dispositius NAS domèstics [4]. Aquests dispositius permeten realitzar còpies de seguretat en una LAN, però no tenen la funció de realitzar còpies de seguretat entre dispositius. Aquests sistemes permeten tenen una solució semblant a la que es proposa en aquest article, però en comptes de fer les còpies entre dispositius iguals de ma-

nera gratuïta, permet fer les còpies en remot a servidors privats amb un cost en funció del espai que precisa l'usuari.

La solució que es proposa en aquest article és una alternativa a les còpies de seguretat en remot que existeixen actualment i que són de pagament. Les còpies en remot es realitzarien en servidors particulars a canvi de cedir espai en el nostre servidor. D'aquesta manera podem tenir còpies de seguretat de la informació del servidor domèstic en un servidor remot assumint només el cost dels dispositius per emmagatzemar les dades.

4 METODOLOGIA

En aquest projecte la metodologia que s'ha seguit per assolir els objectius és la del procés iteratiu [5]. S'ha dividit el projecte en diverses etapes, i en cada etapa s'han realitzat les parts d'anàlisi de requisits, disseny, implementació i proves. D'aquesta manera, al finalitzar una etapa es tenia un punt de retorn en cas de tenir complicacions en alguna part del projecte.

Periòdicament han hagut reunions entre el tutor i l'alumne del projecte i s'ha exposat la feina realitzada. En cada reunió s'ha fet un anàlisi del progrés del projecte i s'han marcat els objectius per la següent reunió.

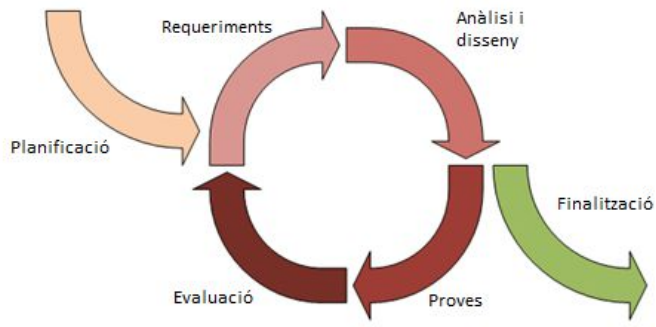

Figura 3. Procés iteratiu. Metodologia utilitzada durant el projecte.

S'ha escollit aquesta metodologia perquè durant el projecte no es tenia present fins a quina funcionalitat hi hauria temps a implementar, i mitjançant el procés iteratiu es podien anar tancant fases del projecte.

5 DESENVOLUPAMENT

En aquesta secció es presenta la part de desenvolupament del projecte. Aquesta secció ha estat dividida en les següents subseccions: Anàlisi de les tecnologies que es poden integrar en la nostre solució, anàlisi de requisits del sistema, disseny del sistema, implementació del sistema, proves realitzades i anàlisi de resultats.

5.1 Anàlisi de les tecnologies que es poden integrar en la nostre solució

En aquesta secció s'analitzen les diferents tecnologies existents que es poden utilitzar per al desenvolupament del nostre sistema. A continuació s'exposen les diferents tecnologies analitzades així com les seves llicències.

- Rsync: Aquesta tecnologia permet realitzar còpies entre diferents directoris (local i remot) copiant només la informació que ha estat modificada respecte la última còpia de seguretat [6]. Es troba disponible sota llicència *GNU General Public License versió 3*.
- SSH: Ens permet establir connexions xifrades entre els servidors. OpenSSH està disponible sota llicència *OpenBSD Copyright Policy*.
- VSFTPD: Permet crear un servidor FTP per al transport de fitxers entre els dos servidors. Aquesta tecnologia està disponible sota llicència *GPL*.
- Navegador web: Podem utilitzar un navegador web, com per exemple, el navegador Firefox, com a interfície per a gestionar el sistema a desenvolupar.
- Duplicity: Aquesta tecnologia permet realitzar còpies de seguretat xifrades en local o en remot. Utilitza *librsync* per realitzar còpies incrementals de només els fitxers que s'han modificat des de la última còpia [7]. La llicència d'aquest software és *GNU GPL v2*.

Aquestes tecnologies amb els tipus de llicències que disposen poden ser utilitzades per a desenvolupar el nostre sistema. A continuació es llisten les diferents propostes que ens permeten integrar les tecnologies analitzades en el projecte. del nostre sistema.

- Proposta 1: Utilitzar *rsync* per la sincronització i còpia de fitxers entre el servidor local i el remot. Aquesta tecnologia és eficient amb l'ús de recursos ja que només copia els fitxers nous i els que han estat modificats respecte la última còpia. El problema d'aquesta tecnologia és que no permet xifrar la informació en el servidor remot.
- Proposta 2: Tenir la informació del sistema de fitxers duplicada. Per una banda tenir la informació sense xifrar, i per altre banda, tenir-la xifrada en el servidor local. A mesura que s'apliquen canvis en la informació sense xifrar, anar actualitzant la informació duplicada xifrada. En el moment de fer la còpia de seguretat, mitjançant *rsync* podríem fer còpies de seguretat de la informació xifrada al servidor remot. D'aquesta manera es copiaria només la informació modificada i la còpia en remot seria xifrada. Aquesta opció té un problema de gestió de espai en local. Estaríem ocupant el doble de espai en el sistema de fitxers local.
- Proposta 3: Aquesta proposta es basa en xifrar les dades durant el procés de còpia de seguretat. D'aquesta manera la informació en remot s'emmagatzema xifrada i no és necessari tenir la informació duplicada en el sistema local. En aquest cas, no seria possible utilitzar *rsync* per el mateix motiu que en la proposta 1. Les dades entre el servidor local i el remot serien diferents (degut al xifrat) i aquesta tecnologia no funcionaria.
- Proposta 4: Aquesta proposta consisteix en l'ús de la tecnologia *duplicity* per realitzar les còpies de seguretat. Amb aquesta tecnologia és possible treballar amb el protocol FTP per el transport de fitxers i SSH per establir les connexions de manera segura.

Aquesta tecnologia treballa amb *librsync* que permet realitzar còpies incrementals xifrades.

Proposta	Xifrat	Eficient	Recursos mal gestionats
1	No	Si	----------
2	Si	No	Ús de disc local
3	Si	No	CPU i recursos de xarxa
4	Si	Si	----------

Taula 1. En aquesta taula es resumeixen les avantatges i els inconvenients de cada proposta realitzada.

Després d'analitzar les diferents tecnologies i realitzar un estudi de com podem integrar-les en el nostre projecte, ens quedem amb les tecnologies esmentades en la proposta 4 per implementar la part de realitzar de còpies de seguretat entre els servidors local i remot.

En aquesta secció s'han proposat les diferents tecnologies que ens poden ajudar en la implementació de la solució proposada i s'ha realitzat un anàlisi de com es poden integrar en el nostre projecte.

5.2 Anàlisi de requisits

En aquesta secció es presenta l'anàlisi de requisits del sistema. Els requisits han estat dividits entre els funcionals i els no funcionals [8]. A continuació es llisten els requisits extrets:

Requisits funcionals:

- Un botó de la interfície ha de permetre al usuari realitzar una còpia de seguretat en el moment que prem el botó.
- Les còpies de seguretat han de ser xifrades amb la clau que especifica l'usuari.
- Un botó de la interfície ha de permetre a l'usuari recuperar tot el sistema de fitxers remot.
- Un input text ha de permetre a l'usuari introduir la clau per desxifrar la informació recuperada del servidor remot.
- Un botó ha de permetre al usuari recuperar un fitxer o carpeta del servidor remot.
- Un input text ha de permetre a l'usuari introduir el fitxer o carpeta que vol recuperar del servidor remot.
- El sistema ha de proporcionar a l'usuari una visió global del sistema de fitxers local complet i del sistema de fitxers remot complet.
- El sistema ha de proporcionar a l'usuari la visió del les còpies de seguretat planificades.
- Mitjançant menús desplegables l'usuari ha de poder planificar noves còpies de seguretat.
- Un botó ha de permetre a l'usuari eliminar una planificació de còpia de seguretat.

Requisits no funcionals:

- El sistema s'ha de poder executar en Raspbian OS.
- La contrasenya per xifrar les dades ha de ser com a mínim de 10 caràcters.
- La contrasenya per xifrar les dades ha de contenir números i lletres.
- El procés de xifrat s'ha de fer en el servidor local, abans de que les dades siguin enviades al servidor remot.
- La interfície d'usuari serà un navegador web.
- En el procés de còpia de seguretat només es tindran en compte els canvis respecte l'última còpia realitzada.
- En el procés de recuperació es desxifrarà la informació utilitzant la clau especificada per l'usuari.

5.3 Disseny del sistema

En aquesta secció es mostra el disseny del sistema implementat. La part del disseny ha estat dividida en tres subseccions: el disseny de realitzar una còpia de seguretat, el disseny de recuperar informació del servidor remot i el disseny de la planificació i gestió de còpies de seguretat.

A continuació es mostra el disseny de la part del sistema que s'encarrega de realitzar una còpia de seguretat. Per realitzar una còpia de seguretat, l'usuari ha de introduir la contrasenya que serà utilitzada per xifrar la còpia. Aquesta mateixa contrasenya serà utilitzada per autenticar-se amb el servidor remot. D'aquesta manera s'aconsegueix que l'usuari sempre xifri les còpies amb la mateixa contrasenya i no tingui problemes a l'hora de desxifrar les còpies realitzades. En cas què la contrasenya que introdueix l'usuari en el moment de realitzar la còpia no sigui correcte, no es podrà autenticar amb el servidor remot i no s'efectuarà la còpia.

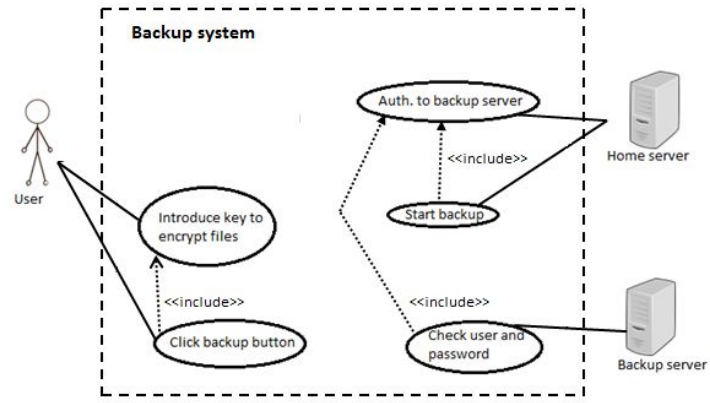

Figura 4. Diagrama de casos d'ús de la part del sistema de realitzar una còpia de seguretat.

Mitjançant un diagrama de seqüència, es permet detectar les diferents accions que es realitzaran i en l'ordre que s'han de produir en un procés de còpia de seguretat. Amb el diagrama de la Figura 5 es mostren les accions que ha de realitzar l'usuari de manera seqüencial en el sistema per a realitzar una còpia de seguretat [9]. També es poden veure les accions que realitzaran els servidors durant aquest procés.

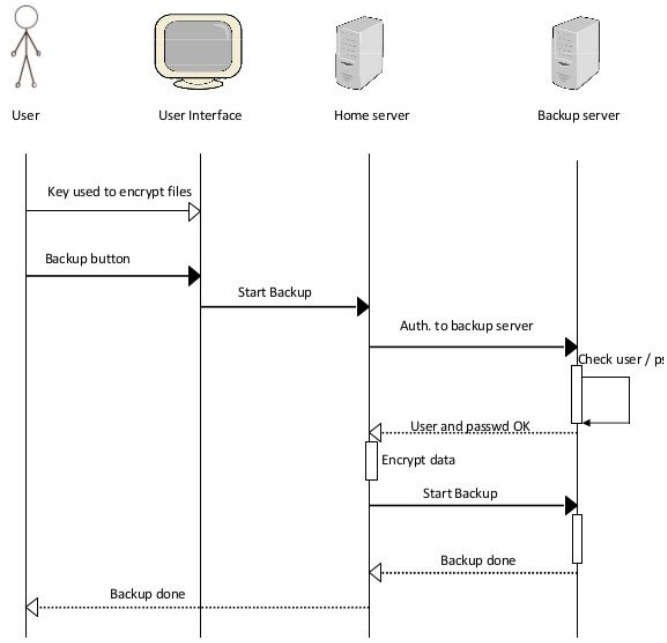

Figura 5. Diagrama de seqüència de la part del sistema de realitzar una còpia de seguretat.

En el següent apartat es mostra el disseny de la part del sistema en què l'usuari pot recuperar informació del servidor remot. En aquest cas, l'usuari ha d'especificar la clau per desxifrar la informació que recuperarà del servidor remot. Seguint la metodologia del disseny anterior, la contrasenya per desxifrar els fitxers és la mateixa que s'utilitza per autenticar-se en el servidor remot. D'aquesta manera evitem possibles errors de l'usuari al intentar desxifrar els fiters recuperats.

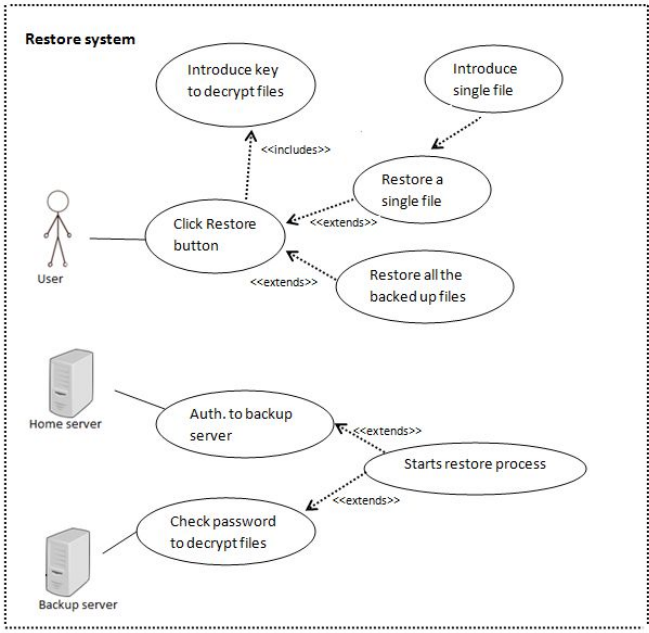

Figura 6. Diagrama de casos d'ús de la part del sistema de recuperar informació del servidor remot.

En aquesta funcionalitat del sistema, l'usuari pot recuperar tot el sistema de fitxers que té copiat en el servidor remot. En cas que ho desitgi, pot recuperar un sol fitxer o carpeta que ha d'especificar manualment i seleccionar la opció de la interfície "Restore a single file". La interfície gràfica li proporciona a l'usuari quins documents es troben en el servidor remot. Aquesta funcionalitat s'explica amb més detall en la següent subsecció.

En el següent apartat es mostra el disseny de la part del sistema que permet a l'usuari gestionar i planificar les còpies de seguretat del servidor local al servidor remot. En el següent diagrama es presenten els diferents casos d'ús que s'han inclòs en el disseny de la part del sistema de la planificació de còpies de seguretat. En aquest disseny s'han de tenir en compte els següents casos d'ús:

- Veure les còpies de seguretat planificades.
- Afegir una nova planificació de còpia de seguretat.
- Eliminar una planificació anteriorment creada.
- Aplicar els canvis que ha realitzat l'usuari utilitzant la interfície de configuració del servidor local.
- Realització de còpies de seguretat en el moment que ha escollit l'usuari.

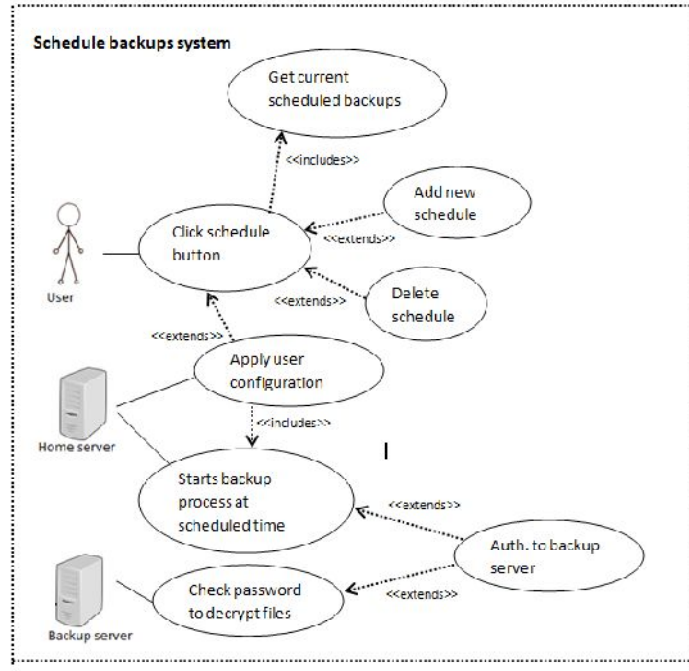

Figura 7. Diagrama de casos d'ús de la part del sistema que permet a l'usuari gestionar i planificar còpies de seguretat.

5.4 Implementació del sistema

En aquesta secció s'expliquen les principals funcionalitats implementades en el projecte. A continuació es llisten aquestes funcionalitats i s'expliquen amb breu detall la forma en que han estat implementades.

Realitzar una còpia de seguretat. Aquesta funcionalitat permet a l'usuari realitzar una còpia de seguretat en el moment que selecciona aquesta opció del sistema.

Recuperar informació del servidor remot. Aquesta funcionalitat permet a l'usuari recuperar dades prèviament copiades. En aquesta funcionalitat l'usuari pot decidir si vol recuperar tota la informació del servidor o només el arxiu o carpeta que especifica manualment.

Mostrar el sistema de fitxers complet del servidor local en el moment que l'usuari entra al sistema. D'aquesta manera l'usuari pot veure quins fitxers es troben en el sistema local. Per implementar aquesta funcionalitat, en el moment que l'usuari carrega la pàgina d'inici del sistema, es realitza una crida a la comanda "*tree*" del sistema operatiu del servidor. Aquesta comanda desplega una vista de tot el sistema de fitxers. Tot seguit, s'emmagatzema el resultat de la comanda en un fitxer de text. Quan l'usuari accedeix al sistema, la interfície mostra el contingut del fitxer de text que conté la vista de tot el sistema de fitxers.

En la Figura 8 es mostra com la interfície del sistema desenvolupat mostra el contingut del sistema de fitxers. Aquest és un sistema de fitxers de prova que s'ha utilitzat durant la implementació del sistema.

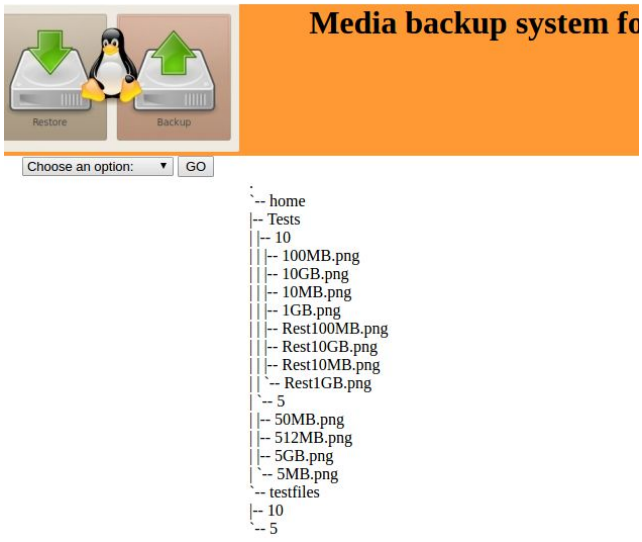

Figura 8. Interfície implementada on es mostra a l'usuari el sistema de fitxers del servidor domèstic.

La següent funcionalitat que es presenta és la de mostrar el sistema de fitxers copiat en el servidor remot. Aquesta funcionalitat mostra una vista del sistema de fitxers que hi ha en el servidor remot en el moment que l'usuari accedeix a la pàgina de recuperació d'informació. D'aquesta manera l'usuari pot consultar quina informació pot recuperar del servidor de còpies de seguretat. Per implementar aquesta funcionalitat el que s'ha realitzat és llençar la comanda "*tree*" en el sistema operatiu local just després de que s'hagi produït una còpia de seguretat sense errors. A continuació s'emmagatzema la sortida de la comanda en un fitxer de text i quan l'usuari accedeix a la pàgina de recuperació d'informació, es mostra el contingut del fitxer de text. D'aquesta manera, en cas que l'usuari tingui la necessitat de recuperar un sol fitxer del sistema remot, mitjançant aquesta funcionalitat, podrà veure a quin directori es troba el fitxer per introduir-lo com a paràmetre a la interfície i recuperar les dades que necessita. En la Figura 9 es mostra una captura de pantalla de la interfície implementada. A la part esquerre de la interfície es veuen els paràmetres que ha d'introduir l'usuari per poder iniciar el procés de recuperació. A la part dreta de la interfície es mostren els fitxers copiats en el directori remot.

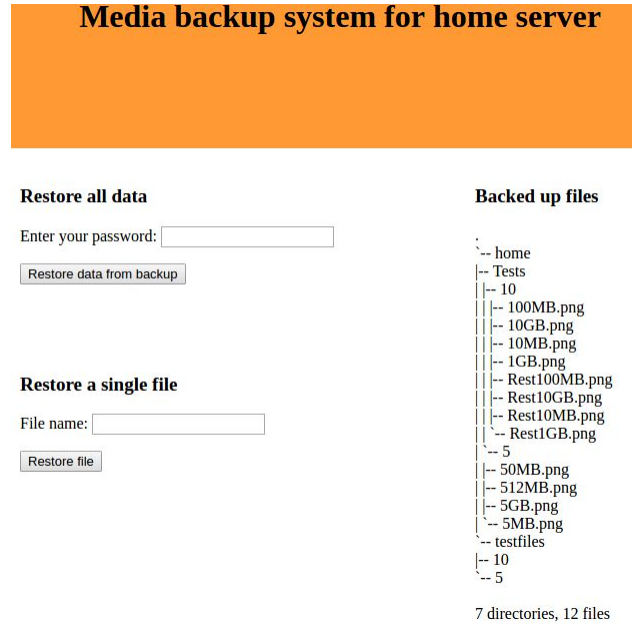

Figura 9. Interfície implementada on es mostra a l'usuari el sistema de fitxers del servidor remot.

Gestió i planificació de còpies de seguretat. Aquesta funcionalitat permet a l'usuari planificar còpies de seguretat perquè es realitzin en el moment que especifica i també permet configurar còpies de seguretat rutinàries. Per a aquesta implementació s'ha utilitzat *cron*[1]. Per a aquesta funcionalitat s'ha implementat una interfície que li permet al usuari treballar amb *cron* de manera amigable i fàcil de la següent forma. Quan l'usuari accedeix a la pàgina de configuració de còpies de seguretat se li mostren les còpies que hi ha actualment configurades. Això es fa mostrant la informació de l'arxiu de configuració del *cron*. En la pàgina de configuració de còpies l'usuari pot afegir una nova planificació de còpies de seguretat on, mitjançant la interfície, introdueix la configuració que vol aplicar. Aleshores, el sistema filtre les dades de la interfície i les adapta al format corresponent pel *cron*. A continuació, afegeix les dades adaptades al fitxer de configuració. Finalment, el sistema fa una crida al *cron* important el nou fitxer per aplicar els canvis.

En la mateixa pàgina de configuració l'usuari també pot eliminar les planificacions realitzades. Per realitzar aquesta acció, s'utilitza un desplegable on l'usuari ha d'introduir el número de la llista que pertany a la planificació de còpies de seguretat que vol eliminar i seleccionar la opció "Delete schedule". Aleshores el sistema cerca a l'arxiu de configuració la planificació especificada per l'usuari, l'elimina i torna a importar la nova configuració per aplicar els canvis.

En la Figura 10 es mostra una captura de pantalla de la interfície que permet realitzar les accions descrites en aquesta secció.

[1] Cron és un administrador de processos en sistemes Unix que executa els processos especificats en la hora que es configura.

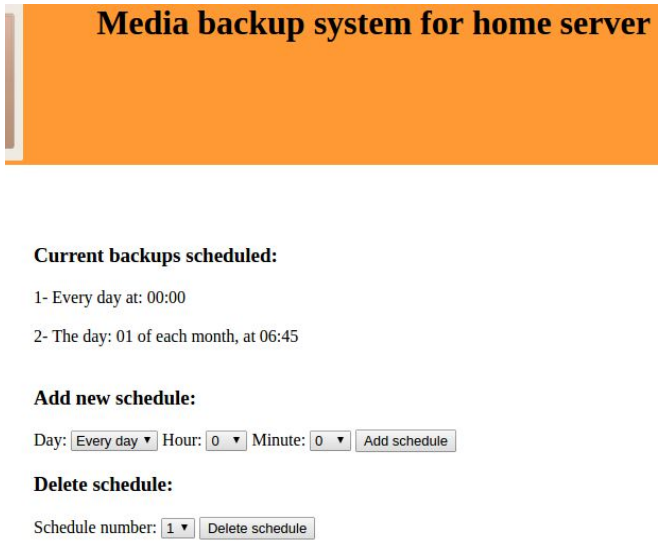

Figura 10. Interfície implementada que permet a l'usuari planificar còpies de seguretat.

A continuació es compara la informació que mostra el sistema a l'usuari, la informació que conté el fitxer de configuració del cron i la configuració importada del fitxer al cron.

En els tres casos hi ha la mateixa informació, però es pot apreciar un canvi de format en la forma en que es mostra la informació. En la interfície implementada s'adapta el format del cron al llenguatge natural de les persones.

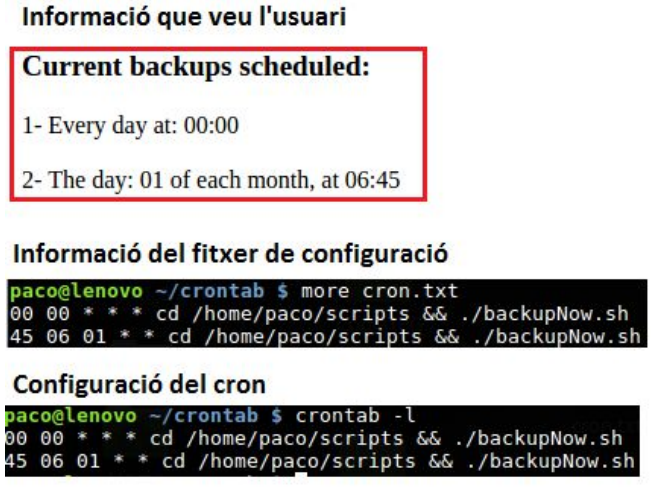

Figura 11. Diferents vistes de les còpies de seguretat planificades. La vista que té l'usuari del sistema de les còpies planificades, la informació adaptada en format cron i, finalment, la configuració aplicada al cron.

En aquesta secció s'han exposat les principals funcionalitats implementades en el projecte. En el següent apartat es veuran les proves que s'han realitzat amb les funcionalitats explicades anteriorment.

5.5 Proves realitzades

En aquesta secció es presenten les proves realitzades amb el sistema implementat. Aquestes proves es divideixen en proves de funcionament i proves de rendiment.

5.5.1 Proves de funcionament

En aquesta secció es mostren les proves de funcionament del sistema i es mostren els resultats obtinguts d'aquestes proves. En la Taula 2 es mostren les funcionalitats provades i la gestió d'errors desenvolupada i integrada en el sistema implementat.

Funcionalitat provada	Resultat	Comentaris
Realitzar una còpia de seguretat.	OK	----------
Recuperació d'un fitxer o directori.	Millorable	Es permet a l'usuari recuperar un fitxer, però s'ha d'introduir exactament el directori on es troba el fitxer que vol recuperar [2].
Recuperació de tot el sistema de fitxers.	OK	----------
Planificació de còpies de seguretat.	OK	----------

Taula 2. Taula on es mostra el resultat obtingut de les funcionalitats provades.

La gestió d'errors implementada es centra en evitar problemes en els processos de còpia i restauració d'informació. Per aquest motiu, aquesta gestió d'errors s'aplica abans de realitzar la connexió amb el servidor remot, ja sigui per realitzar còpies de seguretat o per realitzar accions de recuperació de dades. En funció de l'error que s'ha produït al intentar connectar-se al servidor, el sistema mostra un missatge al usuari. En cas que no hi hagi cap problema amb la connexió es permet que es realitzin les accions que l'usuari sol·licita. Els casos que controla el gestor implementat són:

- El camp usuari o contrasenya no conté dades.
- L'usuari introduït no existeix.
- La contrasenya introduïda no és correcte.
- No és possible establir connexió amb el servidor de remot.

En cas que es produeixi un error que no sigui qualsevol dels mencionats, es mostra un missatge de error al usuari amb el codi del error, perquè pugui reportar el problema.

En aquesta secció s'han vist les diferents funcionalitats provades i la gestió d'errors implementada. En la següent secció es presenten les proves de rendiment que s'han realitzat.

[2] La proposta per millorar el resultat d'aquesta part del sistema és la implementació de una funcionalitat en la interfície d'usuari que permetin recuperar un sol fitxer o directori de manera fàcil per als usuaris.

5.5.2 Proves de rendiment

En aquesta secció es mostren les proves de rendiment realitzades en el sistema. Les proves realitzades consisteixen en la realització de còpies de seguretat de diferents quantitats d'informació i la recuperació de les dades copiades. Aquestes proves s'han realitzat en dos entorns diferents. El primer entorn, d'ara a endavant entorn 1, és una connexió LAN amb un router entre les dues màquines que té un ample de banda de 100 Mbits per segon i una latència mitjana de 0,5 ms entre els dos servidors utilitzats per fer les proves. En aquest entorn es pretén posar a prova el sistema sense restriccions de latència ni ample de banda i s'han mesurat els temps que ha trigat el sistema en realitzar les accions. Els resultats de les proves en aquest entorn es presenta a la Taula 3.

Mida de les dades	Procés de còpia de seguretat	Procés de recuperació de dades
1 MB	1,6	1,1
10 MB	3	2,2
100 MB	14,9	12,7
1 GB	145	137
10 GB	1467	1464

Taula 3. Temps en segons que ha trigat el sistema en realitzar cada acció provada amb un ample de banda de 100 Mbits per segon i una latència.

En el segon entorn, d'ara a endavant entorn 2, s'utilitza la mateixa infraestructura física, però es limita l'ample de banda de les interfícies dels servidors i s'incrementa la latència. En aquest entorn cada servidor té una limitació de 50 Mbits per segon de ample de banda i una latència de 50 ms. En aquest cas, es pretén provar el funcionament del sistema amb restriccions de xarxa i en un escenari més proper a la realitat. En la Taula 4 es mostren els resultats obtinguts d'aquestes proves.

Mida de les dades	Procés de còpia de seguretat	Procés de recuperació de dades
1 MB	6,5	5,5
10 MB	8,4	6,7
100 MB	31,7	28,2
1 GB	279	260
10 GB	2665	2582

Taula 4. Temps en segons que ha trigat el sistema en realitzar cada acció provada.

En aquesta secció s'han vist les proves realitzades amb el sistema i els resultats obtinguts en aquestes proves. En el següent apartat s'analitzen aquests resultats.

5.6 Anàlisi de resultats

En aquesta secció es presenta un anàlisi dels resultats obtinguts en el projecte. En la Gràfica 1, es presenta una comparació entre els resultats obtinguts en fer còpies de seguretat i en recuperar dades en l'entorn 2.

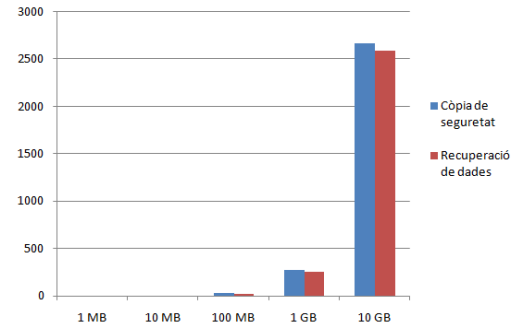

Figura 12. Gràfica on es mostra una comparació en el temps entre el procés de fer còpies de seguretat i el de recuperar dades amb les diferents mides de dades provades.

La diferència de temps entre els dos processos és mínima. A més, a mesura que s'incrementa la quantitat de dades a copiar, la diferència de temps es manté estable i és sempre molt petita entre els dos processos. A continuació es presenta el increment de temps en funció de la mida de les dades a copiar en els dos entorns de prova.

Mida de les dades	50 Mb/s	100 Mb/s
1 MB	0	0
10 MB	22,6%	46,67%
100 MB	73,5%	79,86%
1 GB	88,64%	89,72%
10 GB	89,53%	90,11%

Taula 5. Increment del percentatge de temps que triga en fer-se una còpia de seguretat quan es multiplica per 10 la mida de la còpia de seguretat a realitzar.

En quantitats de dades petites quan es multiplica per 10 la mida de les dades no es multiplica per 10 el temps de còpia de seguretat, sinó que incrementa en menys percentatge. En canvi, com més gran és la quantitat de dades a copiar, més s'incrementa el percentatge de temps. En els nostres casos de prova, a partir de 1 GB de dades, el percentatge incrementa un 90% aproximadament quan es multiplica per 10 les dades a copiar. Aquest factor ens indica que per fitxers més petits de 1 GB el sistema respon millor que amb fitxers grans on el temps de còpia es multiplica pràcticament en la mateixa magnitud que la mida de les dades a copiar. Si multipliquem per 10 la mida de la còpia, es multiplica per 9 el temps. En la gràfica 2 es mostra aquest factor comentat.

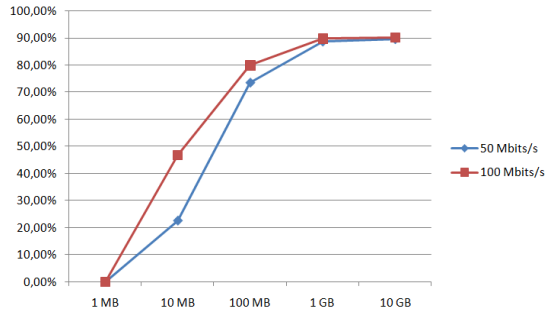

Figura 13. Evolució del increment del temps quan es multiplica per 10 la quantitat de dades a transmetre.

Finalment, es compara la diferència en els resultats obtinguts en realitzar còpies de seguretat entre els dos entorns de proves. En la Taula 6 es mostra la diferència de temps en quant a percentatges entre els resultat de l'entorn 1 i l'entorn 2 quan es multiplica per 10 la quantitat de dades a copiar.

Mida de les dades	50 Mb/s	100 Mb/s	Diferència
1 MB	6,5 s	1,6 s	75,38%
10 MB	8,4 s	3 s	64,28%
100 MB	31,7 s	14,9 s	53%
1 GB	279 s	145 s	48%
10 GB	2665 s	1467 s	45%

Taula 6. Diferència entre els resultats obtinguts en l'entorn de proves 1 i l'entorn 2.

Percentualment la diferència entre els dos entorns es minimitza en funció de la quantitat de dades de la còpia que s'ha de realitzar. Aquest factor es produeix perquè quan s'incrementen les dades a copiar, el sistema triga més en xifrar-les, i el procediment de xifrar genera un coll de ampolla en el procés de còpia de seguretat i provoca una compensació entre la diferència d'ample de banda i de latència entre els dos entorns. Aquest factor es pot observar a la Gràfica 3.

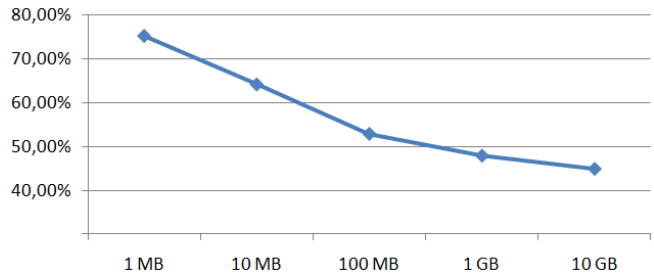

Figura 14. Decrement de la diferència en percentatge entre els resultats obtinguts en l'entorn 1 i l'entorn 2.

6 CONCLUSIONS

En aquesta secció es presenten les conclusions extretes de la realització del projecte de manera crítica i objectiva. Posteriorment es fa una valoració dels aspectes no tractats i un estudi de les possibles extensions del projecte.

Les conclusions extretes del projecte són les següents:

- En primer lloc, es conclou que s'ha assolit l'objectiu principal del projecte, ja que s'ha aconseguit desenvolupar un sistema que permet fer còpies de seguretat entre servidors domèstics i s'han implementat les funcionalitats inicialment planificades.
- En segon lloc, es conclou que el sistema ha respòs de manera correcte a les proves de funcionament realitzades, executant de la manera esperada les funcionalitats implementades.
- Després dels resultats analitzats en la secció anterior, es conclou que el sistema treballa molt bé quan gestiona còpies de seguretat i realitza processos de recuperació amb quantitats de dades de fins a 1 GB.
- També s'arriba a la conclusió que el sistema permet treballar amb grans quantitats de dades, com s'ha pogut veure en les proves de rendiment. Però quan la mida de les còpies de seguretat és superior a 1 GB, el temps que triga en realitzar un procés de còpia o recuperació creix en la mateixa proporció que la quantitat de dades a copiar o recuperar.
- Hi ha aspectes de la interfície gràfica que es poden millorar. La interfície gràfica d'usuari permet realitzar les funcionalitats implementades, però hi ha casos com el de mostrar el sistema de fitxers del servidor o la funcionalitat de recuperar un sol fitxer, que la interfície podria incorporar més funcionalitats i millorar la qualitat del sistema.
- Tot i que s'han implementat les funcionalitats planificades i s'ha assolit l'objectiu principal del projecte, si es volgués posar en producció el sistema desenvolupat, encara hi ha aspectes que es poden integrar i que deixerien el sistema llest per ser posat en producció..

6.1 Possibles extensions

En aquesta secció es realitza un estudi de les possibles extensions i línies de futur del projecte. Després del treball realitzat es considera que aquest projecte es podria continuar desenvolupant en dues tendències diferents. La primera és la de posar el sistema desenvolupat en producció i la segona estaria enfocada a la recerca i investigació de noves solucions i tecnologies per la realització de les còpies de seguretat entre servidors domèstics.

Per a posar el sistema desenvolupat en producció hi ha una sèrie de aspectes que s'haurien de resoldre i que no han estat tractats en aquest projecte per falta de temps. Els principals aspectes destacats que s'haurien d'implementar per poder posar el sistema en producció serien:

- La gestió del la configuració de les direccions IP. Per tal de poder establir connexions entre els servidors domèstics s'hauria de gestionar el problema de resoldre les IPs origen i destí dels servidors. Aquest aspecte té especial importància ja que actualment cada cop més proveïdors de serveis utilitzen assignació d'IPs dinàmiques, fet que complicaria aquest problema i s'hauria de recorre a tecnologies com DNS o realitzar una recerca de un sistema gratuït que ens permeti trobar una solució a aquest problema.
- Solucionar el aspecte del NAT. Donat que aquest sistema estar pensat per servidors domèstics, en la majoria de casos hi haurà routers implementant NAT entre els servidors que es volen fer còpies de seguretat mútuament. Per la realització de proves s'ha realitzat una configuració manual dels routers on hi havia NAT, però abans treure el sistema a producció és un aspecte que es considera important de tractar.
- Gestió d'errors durant els processos de còpia de seguretat. En aquest projecte s'han gestionat els errors principals que es poden produir en el sistema, però no s'han tractat els errors que es puguin produir per

una caiguda de un dels sistemes durant el procés de còpia de seguretat.

En referència a la recerca de noves tecnologies que permetin fer còpies de seguretat entre servidors domèstics, després de la implementació d'aquest sistema es consideren interessants les següents línies de recerca:

El desenvolupament de una xarxa P2P descentralitzada entre diferents servidors domèstics. La idea seria semblant a la solució que es proposa en aquest article, on cada node de la xarxa tindria una partició per emmagatzemar la seva pròpia informació, i una partició per a posar en disposició de la xarxa P2P. En aquest entorn, les còpies estarien distribuïdes entre els diferents nodes de la xarxa de tal manera que en cas de la caiguda de un node, es perdria molt poca informació. Si a més, el sistema desenvolupat realitzés les còpies de seguretat amb informació duplicada, es podria evitar la pèrdua d'informació quan un node de la xarxa caigués.

Estudi dels algoritmes de xifrat que s'utilitzen per xifrar les còpies de seguretat. En aquest projecte no s'ha realitzat un estudi del xifrat que utilitza el sistema desenvolupat, i per tant, potser hi ha algoritmes que s'adapten millor a la solució que es planteja en aquest article. En aquest estudi es podria cercar la millora el sistema en dos sentits. Per una banda, cerca un algoritme de xifrat que permeti reduir el temps que triga el sistema en xifrar i desxifrar les dades per aconseguir millorar el temps obtingut en els processos de còpia i restauració de dades. Per altre banda, es pot realitzar un estudi sobre la seguretat del xifrat que s'utilitza actualment i cercar l'algoritme que més seguretat proporcioni a les còpies realitzades en remot.

Agraïments

En aquesta secció s'exposen els agraïments a les persones que d'alguna manera han col·laborat en el projecte. Aquest projecte no hauria estat possible sense el suport, la col·laboració i la dedicació d'aquestes persones.

En primer lloc, es vol agrair al tutor del treball, el Dr. Sergi Robles, la ajuda que ha proporcionat en la realització d'aquest. La seva aportació en quant a crítiques, consells i recomanacions que han sigut indispensables per al desenvolupament del projecte, així com la seva permanent disposició a ajudar i resoldre dubtes que han anat sorgint en les etapes més difícils del treball.

També es vol agrair a Florin Lohan la seva participació en les fases inicials del projecte, aportant idees de com es podia enfocar la solució que es pretenia desenvolupar.

A tot el col·lectiu universitari, professors i alumnes que directe o indirectament han participat en fer possible la realització del treball.

Finalment, agrair a la família i amics el seu recolzament durant el període de temps que ha durat aquest projecte.

Bibliografia

[1] Brad Nisbet, Laura DuBois. 2011. The benefits of cloud-based backup: Addressing Business Continuity in a Distributed Workforce. Whitepaper.

[2] A Forrester Consulting Thought Leadership Commissioned By Microsoft. 2014. Cloud Backup And Disaster Recovery Meets Next-Generation Database Demands. Whitepaper.

[3] Amazon Web Services. 2016. Backup and Recovery Approaches Using AWS. Whitepaper.

[4] IBM Storage Networking. 2001. Demystifying Storage Networking DAS, SAN, NAS, NAS Gateways, Fibre Channel, and iSCSI. Paper .

[5] R Pankaj Jalote, Aveejeet Palit, Priya Kurien and V. T. Peethamber. Timeboxing: A Process Model for Iterative Software Development. Journal of Systems and Software, 2004. Paper.

[6] Tridgell, A. and Mackerras, P. 1996. The rsync algorithm. Joint Computer Science Technical Report Series. The Australian National University. Paper.

[7] Aurélio Santos and Jorge Bernardino. 2014. Open Source Tools for Remote Incremental Backups on Linux: An Experimental Evaluation. Journal of systems integration 2014/3. Paper.

[8] Lawrence Chung, Brian A. Nixon, Eric Yu, John Mylopoulos. 2000. Non-Functional requirements in software engineering. Springer Science + Business Media, LCC, pp 153- 155. Llibre.

[9] Santosh Kumar Swain, Durga Prasad Mohapatra and Rajib Mall. 2010. Test Case Generation Based on Use case and Sequence Diagram. Int.J. of Software Engineering, IJSE Vol.3 No.2. Paper.