Analise de desempenho do compartilhamento de dados utilizando a criptografia AES, do E2EE plugin, no servidor ownCloud

Thiago dos Santos Carvalho, Patrícia Bellin Ribeiro

Curso de Tecnologia em Redes de Computadores - Faculdade de Tecnologia de Bauru (FATEC)
Rua Manoel Bento da Cruz, nº 30 Quadra 3 - Centro - 17.015-171 - Bauru, SP – Brasil

tgo.carvalho@hotmail.com, patricia.ribeiro5@fatec.sp.gov.br

Abstract. *To improve the security of files on computer networks, where it was possible to analyze the second time of each test where a local cloud was developed, presenting a friendly interface. This study aims to analyze the performance of security in data sharing using cryptography. This cloud was configured using the Shell (Bash) Script language, and groups were created to ensure encryption enabled and disabled for testing, providing greater security and better performance for two different devices with network access. It is concluded that the cloud has efficiently and effectively demonstrated the objectives proposed in the work.*

Resumo. *Para melhorar a segurança dos arquivos na redes de computadores, onde foi possível analisar o tempo em segundo de cada teste onde foi desenvolvida uma nuvem local, apresentando de interface amigável. Este estudo tem como objetivo analisar o desempenho da segurança no compartilhamento de dados utilizando criptografia. Essa nuvem foi configurada utilizando a linguagem Shell (Bash) Script, e foram elaborados grupos para assegurar a criptografia habilitada e desabilitada para os testes, fornecendo maior segurança e melhores desempenhos para dois diferentes dispositivos com acesso à rede. Conclui-se que a nuvem demonstrou de forma eficiente e efetiva os objetivos propostos no trabalho.*

1. Introdução

O estudo no campo da criptografia teve seu início anterior as questões relacionadas a área computacional. No período pré-histórico da humanidade, os seres humanos criavam diferentes combinações de símbolos com uma escrita secreta, mas com o passar dos anos, as pessoas criaram métodos de codificação. De acordo com Prichett (1987), como a cifra de Ceasar, onde Julius Ceasar escreveu uma mensagem para Marcus Cicero, utilizando um código para modificar todo o alfabeto, substituindo a atual letra por 3 letras a frente. Logo depois com o avanço computacional iniciado no final do século XX, fez com que a criptografia evoluísse e começasse a ter uma complexidade desdobrada por diferentes linguagens de programação, por exemplo, chave simétrica e assimétrica.

Com isso foram criados diferentes algoritmos como o RSA. Segundo Coutinho (2009), é a criptografia mais explorada no modo de chave pública e a mais utilizada no setor comercial. De acordo com Silva et al (2013), o RSA surgiu dos nomes dos criadores Ronald Rivest, Adi Shamir e Leonard Adleman, e sua segurança tem uma complexidade extensa através da fatoração de números primos, como as chaves de segurança que possui

números que são multiplicados entre si mesmo, compõe ao menos 150 algarismos, que é quase improvável fatorar um número deste tamanho. Em relação ao algoritmo AES, que significa Advanced Encryption Standard. Segundo Graff, Kuehlkamp, Domenech (2013, apud Mathias, 2005), relata que este é o algoritmo padronizado pelo governo dos EUA, por ser o mais seguro, pois exige um tempo e esforço computacional menor, por ser um algoritmo de chave simétrica comparado a algoritmos de chave assimétrica.

Justifica-se que ao descrever a comparação entre o desempenho do upload a respeito da sua velocidade de criptografia e sem criptografia, será possível pontuar melhor a aplicabilidade no campo de segurança de redes. Nesse sentido a importância deste estudo se desdobra em dados que poderão ser utilizados como base para otimização da defesa de arquivos na nuvem aumentando a segurança de redes de computadores.

Considerando a temática retratada no projeto, objetiva-se descrever o desempenho da nuvem privada e analise da velocidade de upload dos arquivos com e sem criptografia.

A temática dessa pesquisa versa sobre complexidade computacional da criptografia. Para a exploração deste tema apresenta-se tópicos essenciais que fundamentarão teoricamente o presente trabalho: seção 1.1 apresentação da pesquisa, seção 1.2 Criptografia, 1.3 Criptografia simétrica, 1.4 Criptografia assimétrica, 1.5 Rivest-Shamir-Adleman (RSA), 1.6 Advanced Encryption Standard (AES), 1,7 Owncloud. Na seção 2.0 é abordado os métodos da pesquisa, apresentando-se os materiais que foram utilizados. Na seção 3.0 os resultados do trabalho. Na seção 4.0 apresenta a conclusão. Na seção 5.0 mostras as referências. Por fim, 6.0 Trabalhos Futuros.

1.2 Criptografia

Ao longo dos anos diversos tipos de criptografias existiram, uma delas e a Cifra de Caesar. De acordo com Prichett (1983), cifra é um sistema que transforma texto simples em texto cifrado, utilizando um agrupamento de transformações a cada caractere (ou letra) em um texto simples, com isso a cifra de Ceasar, foi constituída quando Julius Ceasar escreveu uma mensagem para Marcus Cicero, utilizando um código para modificar todo o alfabeto, substituindo a atual letra por 3 letras a frente. Logo depois com o avanço das tecnologias e das comunicações, a necessidade de proteger uma mensagem se tornou cada vez maior, através da criação de maquinas com um enorme poder computacional. Segundo Fiarresga (2010), no início da década de 70, as cifras eram todas simétricas sendo a única chave é capaz de encriptar e desencriptar uma mensagem, mas logo depois surgiu a criptografia assimétrica para qual existe 2 chaves uma pública para encriptar e outra privada para desencriptar.

De acordo com Fiarresga (2010), alguns propósitos da criptografia são:

- Confidencialidade, onde tem o objetivo de guardar todo o conteúdo da informação para todos excetos para as pessoas que tenham acesso a ela.
- Integridade da informação – assegura que não há modificação independente da intenção.
- Autenticação de informação - serve para detectar pessoas ou processos na comunicação estabelecida.
- Não repudiação – impedir que qualquer uma das partes comprometida na comunicação contradite o envio ou a entrada de uma informação.

1.3 Criptografia simétrica

Sendo um dos métodos de cifragem mais utilizados, segundo Carvalho (2008), a empregabilidade da criptografia simétrica é possui apenas uma chave, que envia ou armazena uma mensagem para um algoritmo e com isso é a mensagem criptografada é enviada e somente quem possuir a chave secreta pode decodificar a mensagem.

Segundo o site InfoWester (2009), alguns dos algoritmos que usam a simétrica é o AES (Advanced Ecryption Standard) é um dos algoritmos mais conhecidos, confiável e compatível com diversos sistemas operacionais. Mesmo sendo um algoritmo seguro possui algumas desvantagens. sendo uma delas a quantidade de chaves distribuídas, caso tenha muitas pessoas e empresas envolvidas, e o meio de comunicação pode não ser seguro e cair em mãos erradas.

Na Figura 1 é esquematizado o método utilizado pela criptografia simétrica, criptografando uma mensagem através de uma chave, sendo que a mensagem criptografada utiliza a mesma chave para descriptografar.

Figura 1: Codificação da chave simétrica. Elaboração de Carvalho (2008).

1.4 Criptografia assimétrica

Sendo um dos métodos mais seguros atualmente, Carvalho (2008), esclarece que existem duas chaves, uma pública e outra privada, para codificar e decodificar. Com isso somente o dono deverá ter a chave privada. Desta forma cada mensagem codificada com a chave pública pode ser exclusivamente decodificada com a chave privada e vice-versa. Segundo Costa (2008), isso exige a necessidade de um meio confiável de comunicação e transferência de dados.

Na Figura 2 é apresentado o método utilizado pela criptografia assimétrica, onde é criptografado uma mensagem através de uma chave, e essa mensagem criptografada deve utilizar uma outra chave para descriptografar.

Figura 2: Codificação da chave assimétrica, utilizando uma chave para a codificação e outra pra decodificação. Elaboração de Carvalho (2008).

1.5 Rivest-Shamir-Adleman (RSA)

De acordo com Silva et al (2013), o RSA foi desenvolvido em 1978 no MIT (Instituto de Tecnologia de Massachusetts) pelos criadores Ronald Rivest, Adi Shamir e Leonard Adleman, onde deu origem ao nome RSA, com isso sua segurança possui uma complexidade extensa através da fatoração de números primos. Citando o NIST (National Institute of Standard and Technology), a chave RSA de 1024 bits não concede uma segurança considerável entre 2011 à 2019, ano do qual foi previsto o fim da segurança pleno para a chave de 2048 bits, isto é, não é sugerido o uso de chave de 1024 bits.

Segundo Okumura (2014), ao longo de 40 anos de RSA, muitos pesquisadores identificaram algumas vulnerabilidades, por exemplo, a implantação do algoritmo, que foram reparadas conforme os anos. Entretanto ele suportou todos os ataques feitos pelos maiores gênios da criptografia conseguiram presumir. Sendo um dos primeiros algoritmos denominado de criptossistemas de chave pública e o único que resistiu durante 30 anos de ataques, se tornou o melhor método para encriptar segurança em e-mail, transação bancaria via internet e autenticação de chamadas telefônicas.

1.6 Advanced Encryption Standard (AES)

De acordo com Trevisan, Sancchi e Sanabria (2013), um dos primeiros algoritmos modelo americano foi DES (Data Encryption Standard), sendo utilizado durante vários anos, logo depois em 1998 foi feito um concurso para a nova versão do Rijndael conhecida como AES. Segundo Graff, Kuehlkamp, Domenech (2013, apud Tanembaum, 2003), a ferramenta AES é um algoritmo de chave simétrica, no entanto pode ser aplicada chaves 128 bits e um tamanho de chave 128, 192 ou 256 bits.

1.7 Owncloud

Segundo o site Owncloud (2018), OwnCloud é um arquivo corporativo na nuvem que pode ser criado pelo servidor. Fornece transparência, segurança e controle fácil que podem ser combinados em um ambiente. Ao mesmo tempo, os usuários podem acessar arquivos corporativos de maneira rápida e fácil de qualquer lugar e de qualquer dispositivo. Isso aumenta a segurança e a produtividade.

De acordo com o site Techtudo (2011), Benefícios do OwnCloud, o usuário pode acessar e controlar os dados da melhor maneira possível. Por outro lado, não utiliza servidores no

mundo como concorrentes. Ou seja, usando um servidor pessoal, os usuários compram e salvam onde sabem.

Esses arquivos podem ser acessados de qualquer dispositivo que execute o Linux, ou até mesmo versões do Windows ou do Mac OS X, bem como plataformas móveis, como iOS e Android.

2.0 Materiais e Método

Para o desenvolvimento desse método, foi elaborada uma pesquisa bibliográfica sobre conceitos computacionais do Owncloud e da criptografia usada E2EE File Sharing, onde foi utilizado o sistema operacional *Linux Ubuntu 18.04*, configurando o código fonte do owncloud através do terminal fornecendo uma grande ênfase em segurança de redes de computadores. Após a instalação do owncloud foi feita toda a configuração da nuvem, onde foi criado os grupos para da usuario e depois instalado a chave da criptografia na ferramenta, através disso foi habilitada a criptografia, para contratação da licença da criptografia E2EE File Sharing, através da loja de plugins disponível na nuvem, depois disso com a criptografia já habilitada, com o servidor, o notebook e o celular conectados no mesmo roteador na mesma rede, foi criado os devidos grupo de usuários sendo ele o (E2EE enabled, sem crip) feito na configuração de administrador do owncloud, para iniciar os testes, que foi realizado com 4 arquivos de diferentes tamanhos, sendo eles 1 PDF de um livro (242075881_Interchange _Fourth_Edition_Student_s) e 3 filmes em mp4 sendo eles(arquivo2 é o filme Tomorrowland, produzido por Brad Bird. arquivo3 o filme Alem da Morte, produzido por Niels Arden Oplev. arquivo o filme Agora e Para Sempre, produzido por Ol Parker.).

Foi utilizado por meio de transmissão a), uma conexão onde o notebook (teste1) utiliza o cabo ethernet conectado em um roteador, que também está conectado ao servidor do ownCloud, utilizando um outro cabo ethernet. Já no meio de transmissão b), a conexão foi realizada com o celular (teste2) conectado pelo Wifi transmitindo para o roteador, que se comunica com o servidor via cabo ethernet.

Foi pensado em elabora um cenário representando a melhor opção de transmissão sendo o Notebook com hardware superior utilizando o cabo ethernet e a pior opção transmissão sendo o Celular com hardware inferior utilizando o Wifi. Na contagem do tempo de cada teste foi utilizado um outro celular com o cronometro em segundos.

Com isso, foi analisado o desempenho do upload do usuário com o notebook através do cabo ethernet, e o celular Android através do Wifi, logo depois foi realizado os testes com a criptografia desabilitada de ambos dispositivos. Conforme na Figura 3 é possível ver o meio de comunicação da rede utilizado nos testes citados acima.

Figura 3: Meio de transmissão utilizado na transmissão dos dados

Fonte: Thiago dos Santos Carvalho

Para realizar a verificação do instrumento utilizado, foi necessário notebook processador Intel Core i5-4200U, 1.60GHz 2.30GHz 4GB de RAM a nuvem Owncloud Enterprise para encriptar os arquivos, sistema operacional Linux Ubuntu 18.04, navegador Celular Android 2x 2.2 GHz Cortex-A73 + 6x 1.6 GHz Cortex-A53 e outra máquina Windows Intel Pentium 4GB de RAM para testes.

Na Figura 4 é exibido o código fonte do ownCloud que foi configurado, no código acima mostra a instalação do ownCloud, a atualização do diretório, logo depois é feito a instalação do mysql-server, php5 e do apache2.

```
root@thiagopc:/home/thiago# wget -nv
https://download.owncloud.org/download/repositories/production/Ubuntu_18.04/Release.
key -O Release.key
root@thiagopc:/home/thiago# apt-key add - < Release.key
root@thiagopc:/home/thiago# echo 'deb
http://download.owncloud.org/download/repositories/production/Ubuntu_18.04/ /' >
/etc/apt/sources.list.d/owncloud.list
root@thiagopc:/home/thiago# apt-get update
root@thiagopc:/home/thiago# apt-get install owncloud-files
root@thiagopc:/home/thiago# apt-get install apache2
root@thiagopc:/home/thiago# apt-get install mysql
root@thiagopc:/home/thiago# apt-get install mysql-server
root@thiagopc:/home/thiago# mysql_install_db
root@thiagopc:/home/thiago# apt-get install mysql-server
root@thiagopc:/home/thiago# mysql_sucure_installation
root@thiagopc:/home/thiago# apt install mysql-server-5.7
root@thiagopc:/home/thiago# apt install net-tools
root@thiagopc:/home/thiago# apt-get install phpmyadmin php-mbstring php-gettext
root@thiagopc:/home/thiago# phpenmod mcrypt
root@thiagopc:/home/thiago# /etc/init.d/apache2 start
root@thiagopc:/home/thiago# apt-get install php4
root@thiagopc:/home/thiago# apt-get update
root@thiagopc:/home/thiago# apt-get install php5
root@thiagopc:/home/thiago# /etc/init.d/apache2 restart
root@thiagopc:/home/thiago# /etc/init.d/apache2 start
root@thiagopc:/home/thiago# locate at /var/www/owncloud/index.html
root@thiagopc:/home/thiago# apt-get install python-software-properties
root@thiagopc:/home/thiago# add-apt-repository ppa:ondrej/php
```

Figura 4: Instalação do owncloud, mysql, apache2 e php5.0

Fonte: Thiago dos Santos Carvalho

Na Figura 5 é apresentado a atualização do php7.0 com a novas atualizações para instalar o ownCloud, que não estava aceitando a versão anterior.

```
root@thiagopc:/home/thiago# apt-get update
root@thiagopc:/home/thiago# apt-get install php5.6
root@thiagopc:/home/thiago# mv owncloud /var/www/html
root@thiagopc:/home/thiago# cd ..
root@thiagopc:/home/thiago# apt-get install php5.6-json php-xml php-mbstring php5.6-
zip php5.6-gd php5.6-sqlite curl libcurl3 libcurl3-dev php5.6-curl php5.6-gd php5.6-intl
php5.6-mcrypt php5.6-imagick php-pear php-xml-parser php5.6-sqlite sqlite mp3info curl
libcurl3-dev zip php5.6-mbstring php5.6-mcrypt php5.6-mysql php5.6-xml
root@thiagopc:/home/thiago# apt-get install php5.6-json php-xml php-mbstring php5.6-
zip php5.6-gd php5.6-sqlite curl libcurl3 libcurl3-dev php5.6-curl php5.6-gd php5.6-intl
php5.6-mcrypt php5.6-imagick php-pear php5.6-sqlite sqlite mp3info curl libcurl3-dev
zip php5.6-mbstring php5.6-mcrypt php5.6-mysql php5.6-xml
root@thiagopc:/home/thiago# sudo apt-get install php5.6-json php-xml php-mbstring
php5.6-zip php5.6-gd php5.6-sqlite curl libcurl3 libcurl3-dev php5.6-curl php5.6-gd
php5.6-intl php5.6-mcrypt php5.6-imagick php-pear php-xml-parser php5.6-sqlite sqlite
mp3info curl libcurl3-dev zip php5.6-mbstring php5.6-mcrypt php5.6-mysql php5.6-xml
root@thiagopc:/home/thiago# config/config.php
root@thiagopc:/home/thiago# config/config.sample.php
root@thiagopc:/home/thiago# apt-get install php-mongodb php-http php-yaml php-
xdebug php-memcached php-memcache php-mailparse php-gnupg php-stomp
libapache2-mod-php7.1 libphp7.1-embed php7.1-cgi php7.1-cli php7.1-dev php7.1-fpm
php7.1-phpdbg php7.1-bcmath php7.1-bz2 php7.1-common php7.1-curl php7.1-dba
php7.1-gmp php7.1-imap php7.1-json php7.1-mbstring php7.1-mcrypt php7.1-mysql
php7.1-odbc php7.1-pgsql php7.1-snmp php7.1-soap php7.1-sqlite3 php7.1-sybase
php7.1-xml php7.1-xmlrpc php7.1-zip php7.1-opcache ph
root@thiagopc:/home/thiago# apt-get update
root@thiagopc:/home/thiago# ifconfig
root@thiagopc:/home/thiago# /etc/init.d/apache2 restart
root@thiagopc:/home/thiago# /etc/init.d/apache2 start
root@thiagopc:/home/thiago# cd ..
root@thiagopc:/home/thiago# apt-get install -y apache2 mariadb-server libapache2-mod-
php7.0     openssl php-imagick php7.0-common php7.0-curl php7.0-gd     php7.0-imap
php7.0-intl php7.0-json php7.0-ldap php7.0-mbstring     php7.0-mcrypt php7.0-mysql
php7.0-pgsql php-smbclient php-ssh2     php7.0-sqlite3 php7.0-xml php7.0-zip

root@thiagopc:/home/thiago# apt install apache2 mariadb-server libapache2-mod-php7.0
openssl php-imagick php7.0-common php7.0-curl php7.0-gd     php7.0-imap php7.0-intl
php7.0-json php7.0-ldap php7.0-mbstring     php7.0-mcrypt php7.0-mysql php7.0-pgsql
php-smbclient php-ssh2     php7.0-sqlite3 php7.0-xml php7.0-zip php-redis php-apcu
```

Figura 5: Atualização das Bibliotecas php7.0

Fonte: Thiago dos Santos Carvalho

Na Figura 6 mostra as novas bibliotecas php7.2, instaladas para a execução do servidor ownCloud.

```
root@thiagopc:/home/thiago# apt-get -y install php7.2 libapache2-mod-php7.2
root@thiagopc:/home/thiago# /etc/init.d/apache2 restart
root@thiagopc:/home/thiago# systemctl restart apache2
root@thiagopc:/home/thiago# apt install mariadb-server
root@thiagopc:/home/thiago# apt-cache search php7.2
root@thiagopc:/home/thiago# apt-cache search php-
root@thiagopc:/home/thiago# apt-get -y install php7.2-mysql php7.2-curl php7.2-gd
php7.2-intl php-pear php-imagick php7.2-imap php-memcache  php7.2-pspell php7.2-
recode php7.2-sqlite3 php7.2-tidy php7.2-xmlrpc php7.2-xsl php7.2-mbstring php-
gettext
root@thiagopc:/home/thiago# systemctl restart apache2
root@thiagopc:/home/thiago# /etc/init.d/apache2 start
root@thiagopc:/home/thiago# cd ..
root@thiagopc:/home/thiago# yum install mod_ssl.i686
root@thiagopc:/home/thiago# apt install mod_ssl.i686
root@thiagopc:/home/thiago# occ maintenance:singleuser –on
root@thiagopc:/home/thiago# maintenance:singleuser --on
```

Figura 6: Atualização das bibliotecas do php7.2 e reiniciar do apache.

Fonte: Thiago dos Santos Carvalho

3.0 Resultados

A seguinte ferramenta que foi utilizada no suporte à administração de redes de computadores, sendo uma nuvem com maior acesso por esta na versão Enterprise do servidor. Como é observado na figura 7, tem-se um menu de opções onde está localizada na pasta Arquivos que é possível selecionar o lugar que deseja acessar, baixar, carregar ou remover seus arquivos, possui também a função de compartilhamento com outros usuários e marcar os arquivos favoritos para o fácil acesso do usuário.

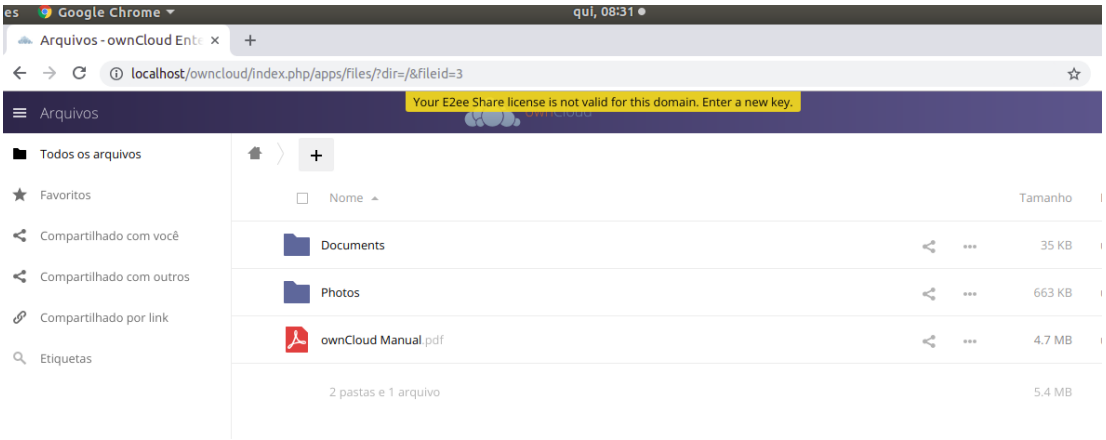

Figura 7. Interface Iniciar do ownCloud ao acessar com seu ID e senha

Fonte: Thiago dos Santos Carvalho

Na figura 8, é exibida a interface de configuração, mostrando todas as opções sendo elas as informações gerais do usuário ou administrador, armazenamento disponível, segurança da nuvem onde é possível habilitar ou não caso esteja com a criptografia ativa, depois é possível observar as opções do administrador onde pode ser feito a aplicação dos plugins, acesso geral dos usuários no servidor, possível armazenamento externo opcional caso habilitado e a criptografia e segurança, onde foi configurado através de uma licença a chave da criptografia na nuvem.

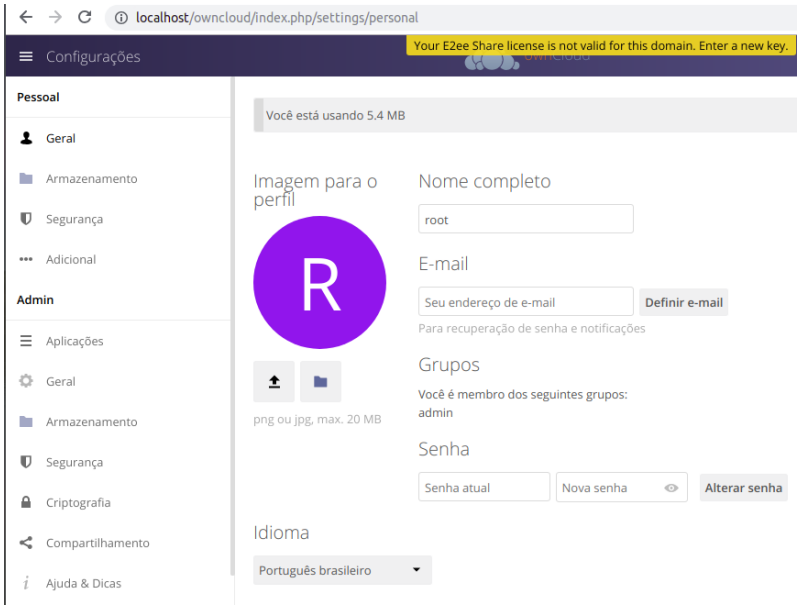

Figura 8. Interface da configuração do Administrador

Fonte: Thiago dos Santos Carvalho

Na figura 9 com a opção criptografia selecionada, é possível observar a licença do plugin de criptografia E2EE Share, onde ela é capaz de fazer criptografias utilizando AES protegendo a chave com criptografia RSA, protegendo os dados do usuário até mesmo do acesso do administrador.

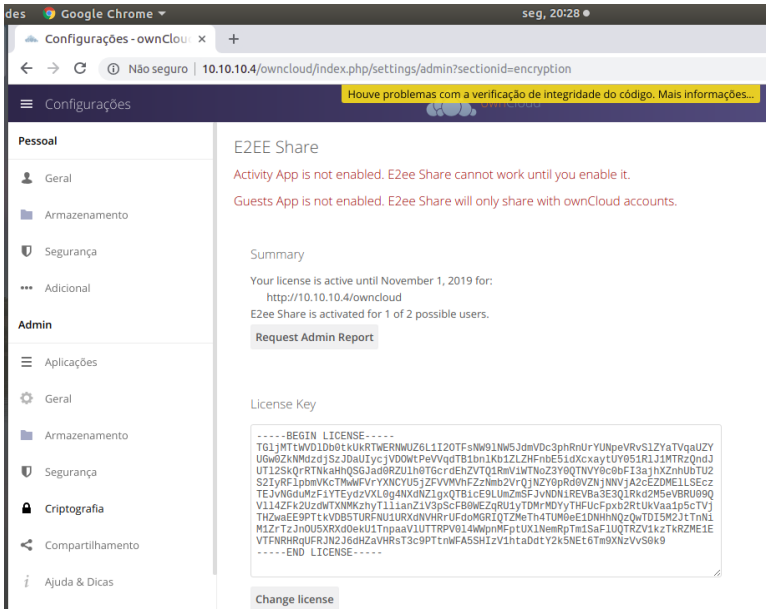

Figura 9. Licença da criptografia

Fonte: Thiago dos Santos Carvalho

Na figura 10 é exibido os usuários que possui acesso a nuvem com nome de cada um dos usuários como (teste1 sendo o Notebook e teste2 o celular Android), com seu determinado grupo controlado pelo administrador que determina o grupo desejado e a quantidade de armazenamento que o usuário tem, que está selecionado o grupo (E2EE enabled) já com a criptografia E2EE Share habilitada.

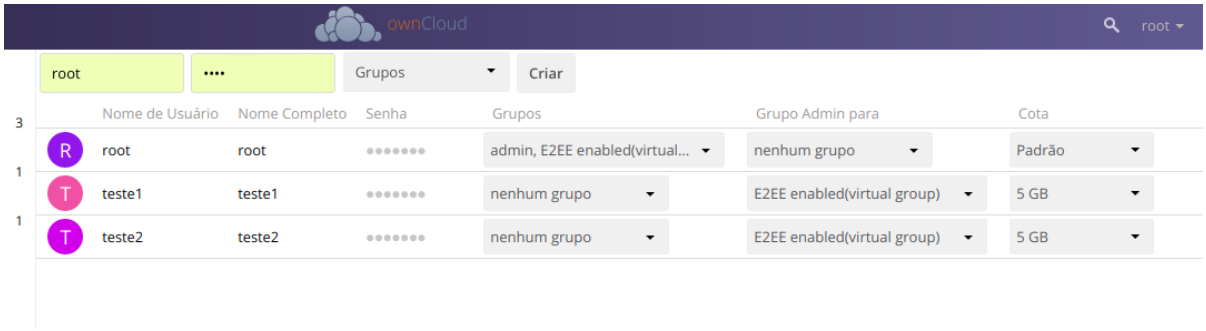

Figura 10. Grupos de usuários com a criptografia habilitada

Fonte: Thiago dos Santos Carvalho

Na figura 11 é apresentado a mesma interface dos grupos de acesso onde os usuários que acessaram a nuvem com o grupo (sem crip) que está com a criptografia desabilitada e limitado com um certo armazenamento e mostrando o acesso a nuvem com nome de cada um dos usuários como (teste1 sendo o Notebook e teste2 o celular Android).

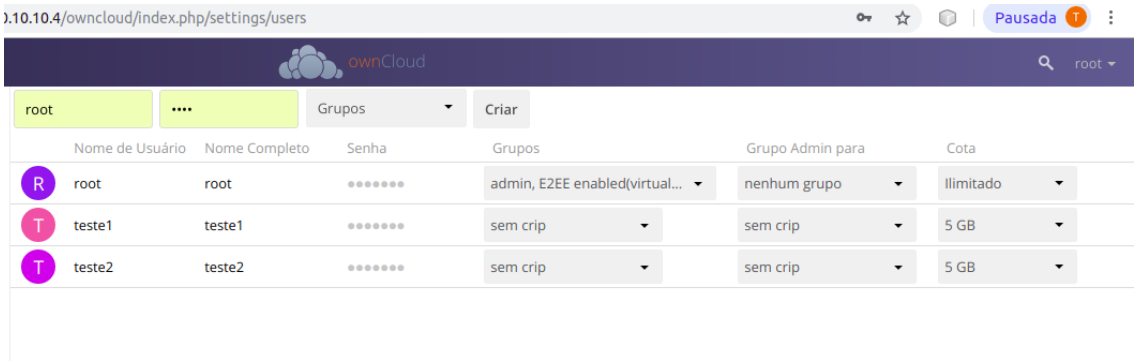

Figura 11. Grupos de usuários com a criptografia desabilitada.

Fonte: Thiago dos Santos Carvalho

Na figura 12 é analisado com resultados obtidos nos testes utilizando o notebook com o cabo Ethernet (melhor opção) apresentando o nome dos arquivos, tipo do arquivo e o tempo em segundos dos testes realizados com e sem a criptografia, e destacando-se a contagem do tempo em segundo de arquivo.

teste1 (Notebook utilizando cabo ethernet)			
NOME E TIPO DOS ARQUIVOS	TAMANHO	COM CRIPTOGRAFIA	SEM CRIPTOGRAFIA
		Tempo em segundos	Tempo em segundos
arquivo1. PDF	58MB	23s	18s
arquivo2. mp4	659MB	230s	152s
arquivo3. mp4	1122MB	705s	425s
arquivo4. mp4	1956MB	1180	838s

Figura 12. Resultados dos testes no Notebook (teste1).

Fonte: Thiago dos Santos Carvalho

Na Figura 13. Apresenta o gráfico dos resultados em tempo em segundo de cada teste realizado no teste (Notebook).

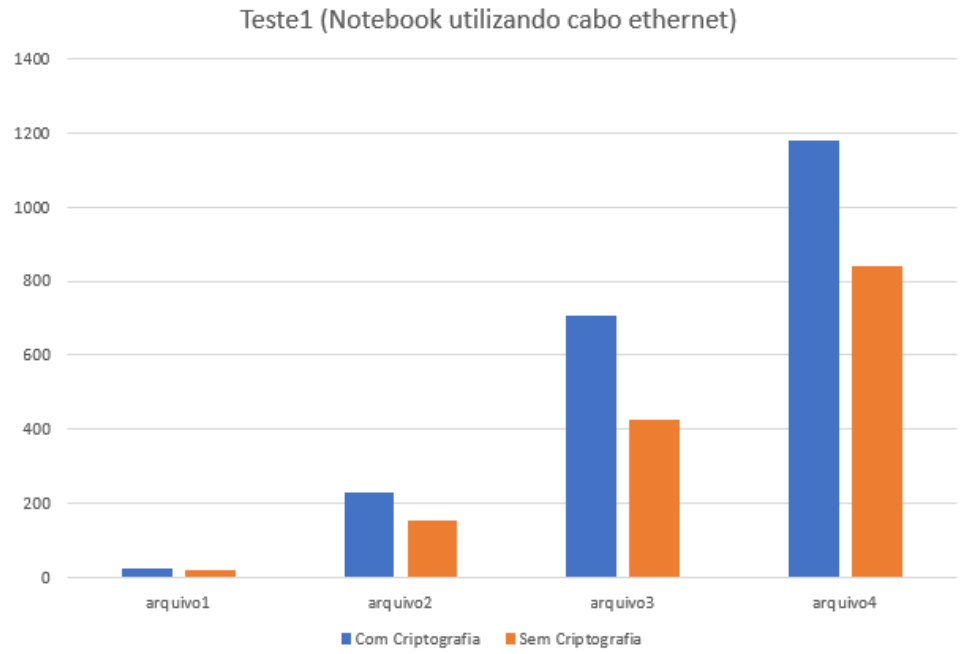

Figura 13: Gráfico dos testes do Notebook(teste1).

Fonte: Thiago dos Santos Carvalho

Na figura 14 é mostrado os resultados alcançados nos testes usando celular Android através do Wifi (pior opção) fornecendo o nome dos arquivos, tipo do arquivo e o tempo em segundos dos testes finalizados com e sem a criptografia habilitada, e também destacando-se a contagem do tempo em segundo de arquivo.

teste2 (Celular utilizando rede Wifi)			
NOME E TIPO DOS ARQUIVOS	TAMANHO	COM CRIPTOGRAFIA	SEM CRIPTOGRAFIA
		Tempo em segundos	Tempo em segundos
arquivo1. PDF	58MB	26s	21s
arquivo2. mp4	659MB	312s	282s
arquivo3. mp4	1122MB	1223s	989s
arquivo4. mp4	1956MB	2924s	1994s

Figura 14. Resultados dos testes no Celular (teste2).

Fonte: Thiago dos Santos Carvalho

Na Figura 15. Apresenta o gráfico dos resultados em tempo em segundo de cada teste realizado no teste2 (Celular).

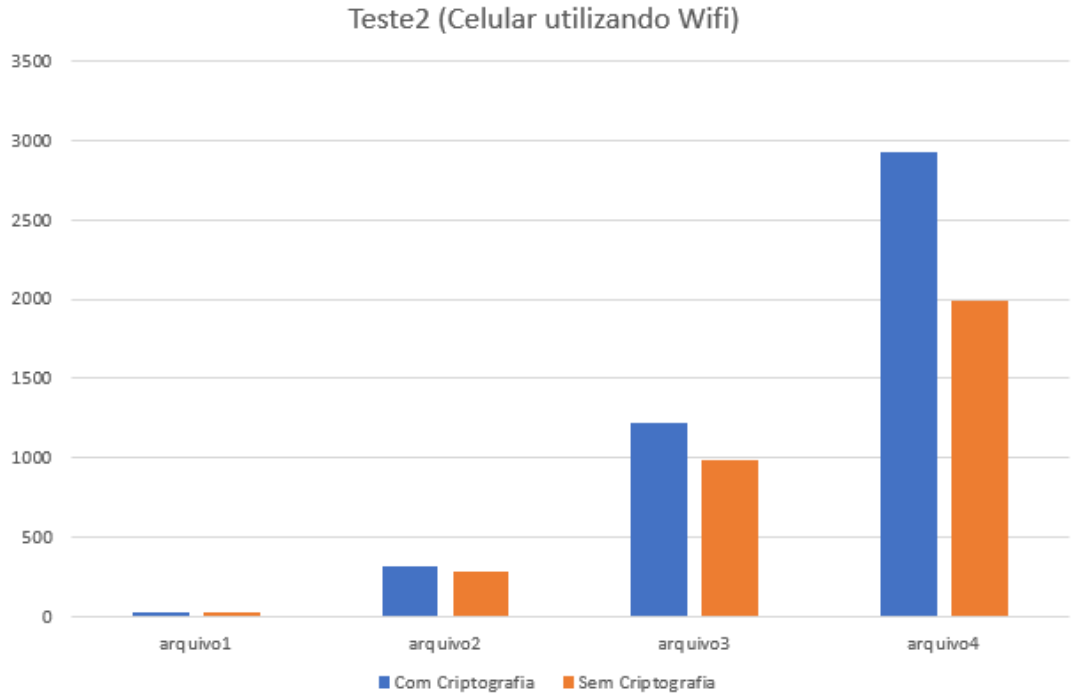

Figura 15: Gráfico dos testes do Celular(teste2).

Fonte: Thiago dos Santos Carvalho

4.0 Conclusão

A nuvem desenvolvida mostrou eficácia nos objetivos propostos no trabalho, oferecendo aos usuários uma interface simples e de fácil acesso utilizando a criptografia habilitada pelo administrador do servidor, para fazer uploads de seus arquivos em segurança.

Com isso, foi possível observar através dos resultados, que o celular (teste2) utilizando a rede através do wifi, sendo a pior opção para transmissão de dados, realizou o upload do arquivo1 e arquivo2 com uma diferença de aproximadamente 13% a mais (tempo em segundos) se comparada a velocidade do upload do notebook (teste1).

Através disso, pode-se concluir que apesar do notebook possuir um hardware mais potente e uma conexão com menor quantidade de oscilação. O celular, devido a evolução tecnologia dos últimos anos, o hardware dele apresentou um excelente resultado, demonstrando qualidade na transmissão de arquivos com tempo imperceptível pelo usuário, apresentando uso favorável do celular, devido a facilidade de acesso do usuário e a velocidade imperceptível em arquivos menores que 700mb, sendo recomendados o uso de notebook para arquivos de tamanhos superiores.

5.0 Referências

Agora e para sempre. Direção: Ol Parker, Produção: Graham Broadbent, Malina Decarlo. Reino Unido: Nancy Richardson Art Jones, 2012.

Alem da Morte. Direção: Niels Arden Oplev, Produção: Laurence Mark, Hassan Taher, Michael Douglas. Estados Unidos: Columbia Pictures, 2017.

Carvalho, H, E. T. (2008). "Trabalho desenvolvido para a disciplina Redes de Computadores II, da UFRJ, no período 2008". https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/hugo/index.html.

Fiarresga, V. M. C. (2010). "Criptografia e matemática". Universidade de Lisboa.

Graff, S., Kuehlkamp, A., & Domenech, M.C. (2013). "Análise da Aplicação da Esteganografia Combinada com o Método Criptográfico AES". Anais do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais.

Gonçalves, L. S & Ribeiro, V. G. (2001). "Um Estudo Comparativo entre algoritmos de criptografia DES – Lucifer (1977) e AES – Rijndael (2000)".

InfoWester (2009). Criptografia. https://www.infowester.com/criptografia.php. Mai.

Okeyinka, A. E. (2015). "Computational Speeds Analysis of RSA and ElGamal Algorithms on Text Data". Proceedings of the World Congress on Engineering and Computer Science.

Okumura, M. K. (2014). Numeros primos e criptografia RSA, Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo.

Owncloud (2018). O ownCloud é a plataforma aberta para mais produtividade e segurança na colaboração digital. https://owncloud.com/. Nov.

Prichett, G. (1983). "Cryptology: From Caesar Ciphers to Public-Key Cryptosystems". The College Mathematics Journal.

Silva, B. et al (2013). Criptografia assimétrica de imagens utilizando algoritmo RSA. Anais do XI CEEL. Universidade Federal de Uberlândia.

Techtudo (2011). Conheça o OwnCloud, o serviço de armazenamento em nuvem privado. https://www.techtudo.com.br/artigos/noticia/2011/10/conheca-o-owncloud-o-servico-de-armazenamento-em-nuvem-privado.html. Out.

Tomorrowland. Direção: Brad Bird, Produção: Brad Bird,Damon Lindelof,Jeff Jensen. Estados Unidos: Walt Disney Pictures, 2015.

6.0 Trabalhos Futuros

Calcular a média do tempo de vários testes ou calcular diferentes tipos de servidores em nuvem.