Penerapan Metode Advanced Encryption Standard pada Sistem Penyimpanan Data Menggunakan Cloud Computing Sebagai Software-as-a-Service

Novira Dwina[1], Nisha Khairani[2], Muhammad Nasir[3*], Indrawati[4]

[1,4] *Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

[1]noviradwina@pnl.ac.id
[2]nisha.khairani@gmail.com
[3*]muhnasir.tmj@pnl.ac.id (penulis korespondensi)
[4]indrawati@pnl.ac.id

Abstrak— **Cloud computing adalah model komputasi yang memungkinkan akses yang mudah dan fleksibel terhadap sumber daya komputasi seperti server, jaringan, penyimpanan, basis data, perangkat lunak, dan layanan lainnya melalui internet. Istilah "cloud" mengacu pada internet itu sendiri, dan *cloud computing* memungkinkan pengguna untuk menggunakan sumber daya ini tanpa perlu memiliki infrastruktur fisik atau perangkat keras secara langsung. Ada beberapa hal yang dapat diterapkan dalam *cloud computing* salah satunya layanan penyimpanan data. Penelitian ini berfokus pada sistem penyimpanan data dengan menggunakan teknologi *cloud computing* untuk dapat mengupload file dari client menuju ke server *ownCloud*. *OwnCloud* merupakan aplikasi platform open-source yang memungkinkan untuk membuat layanan penyimpanan data dan berbagi berkas sendiri di lingkungan cloud. Diperlukan sistem keamanan yang baik dari ownCloud sendiri agar dapat melindungi file yang di upload dari pihak-pihak yang tidak bertanggung jawab (seperti halnya penyadapan) sebelum file tersebut dikirim menuju server. Penelitian ini menggunakan metode *Advanced Encryption Standard* (AES) yang merupakan standar enkripsi yang digunakan secara luas untuk melindungi data sensitif sehingga data yang dikirimkan tidak dapat diubah ataupun dirusak oleh pihak lain. Pengujian enkripsi dan dekripsi dengan algoritma AES kemudian dilakukan pada file txt dan mkv. Hasil pengujian terhadap file yang diuji dengan metode AES dapat terenkripsi dengan benar dan terhindar dari serangan bruteiforceiattack.**
Kata kunci— *Cloud computing, ownCloud, Advanced Encryption Standard*

Abstract— **Cloud computing is a computing model that enables easy and flexible access to computing resources such as servers, networks, storage, databases, software, and other services via the internet. The term "cloud" refers to the internet itself, and cloud computing allows users to use these resources without the need to own the physical infrastructure or hardware directly. There are several things that can be applied in cloud computing, one of which is data storage services. This research focuses on data storage systems using cloud computing technology to be able to upload files from clients to the ownCloud server. OwnCloud is an open-source platform application that allows you to create your own data storage and file sharing services in a cloud environment. A good security system is needed from ownCloud itself so that it can protect uploaded files from irresponsible parties (such as wiretapping) before the file is sent to the server. This research uses the Advanced Encryption Standard (AES) method which is an encryption standard that is widely used to protect sensitive data so that the data sent cannot be changed or damaged by other parties. Encryption and decryption tests with the AES algorithm were then performed on txt and mkv files. The results of testing the files tested with the AES method can be encrypted correctly and protected from brute force attacks.**
Keywords— *Cloud computing, ownCloud, Advanced Encryption Standard*

.

I. PENDAHULUAN

Saat ini media penyimpanan sangat berkembang menjadi penyimpanan online, termasuk pada bagian dari *cloud computing*. Salah satu layanan yang tersedia pada *cloud computing* yaitu *Software-as-a-Service (SaaS).* Pada model layanan ini user atau pengguna dapat memakai aplikasi tersebut tanpa harus mengurus ataupun mengerti layanan yang tersedia seperti pemeliharaan aplikasi atau data yang disimpan, karena hal tersebut merupakan layanan yang sudah tersedia pada SaaS. Salah satu layanan yang disediakan oleh provider untuk pengguna yaitu berupa software *ownCloud* [1]. *SaaS* merupakan adalah model layanan dalam komputasi awan di mana perangkat lunak atau aplikasi disediakan kepada pengguna melalui internet sebagai layanan. Keamanan file dan data pada *ownCloud* masih sangat rentan untuk di serang atau diambil file-nya di database pada server, perkembangan teknologi komputer sekarang semakin canggih maka dalam teknologi informasi dibutuhkan pengamanan data yaitu salah satunya menerapkan algoritma kriptografi yang diyakini lebih kuat dan aman. Dalam penelitin yang akan dibuat terdapat penelitian yang bersangkutan dengan itu peneliti melakukan penelitian terhadap keamanan data yang akan dikirimkan ke ownCloud. Penelitian yang dilakukan oleh Wahyu E.Susanto dengan judul "Pendekatan Keamanan Serta Kecepatan Akses Data Pada *Cloud* dengan Algoritma Huffman Dan AES". bertujuan agar pengguna yakin ketika pengolahan data yang bersifat rahasia mereka dapat disimpan dengan pengamanan hak akses. Mudah tersedia dan fleksibel yang ada dilayanan cloud menyimpan masalah mengenai keamanan data agar dapat berbagi data secara aman, cara mengatasinya yaitu dengan pendekatan berbasis otentik daripada menggunakan pendekatan berbasis komunikasi [2].

Berdasarkan penelitian yang dilakukan sebelumnya maka peneliti akan membahas mengenai pengamanan *ownCloud* yang ada pada *Software As A Service* (SaaS) dengan menerapkan algoritma advanced encryption standard sebagai cipher yang aman dan dapat melindungi informasi atau data

pribadi bersifat rahasia. Algoritma Advanced Encryption Standard (AES) dapat digunakan untuk menjaga data atau informasi agar aman. AES mempunyai ketahanan terhadap berbagai jenis serangan yang sering terjadi pada jaringan komputer [3].

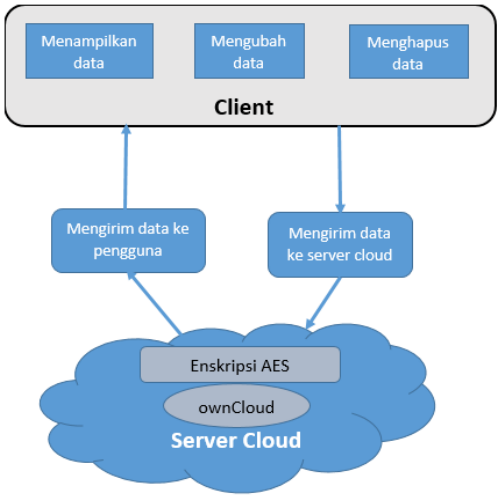
Penelitian ini diselesaikan untuk membuat sistem penyimpanan data menggunakan owCloud dengan Advanced Encryption Standard. Layanan ini dapat diakses untuk public dan public pun tidak perlu khawatir untuk menyimpan data mereka pada *ownCloud* dikarenakan terdapat sistem dimana pada saat client mengupload data atau menyimpan data maka data tersebut langsung dienkripsi dengan metode Advanced Encryption Standard (AES) tersebut. Sistem ini bekerja terus menerus tanpa henti dan secara online melalui jaringan internet. Semua kegiatan akan berpusat pada server dan setiap data-data akan tersimpan langsung dan dapat digunakan setiap saat.

Untuk membuat dokumen lebih aman ketika dikirimkan ke *ownCloud*, penelitian ini melakukan analisis sistem penyimpanan untuk syn client *ownCloud* dengan menerapkan algoritma kritografi Advanced Encryption Standard (AES). Dengan algoritma ini diharapkan pengamanan data dapat lebih terjamin. Pada penelitian ini menggunakan aplikasi *ownCloud* sebagai software yang sudah disediakan[4]. Dengan adanya *ownCloud* dan algoritma Advanced Encryption Standard (AES) bertujuan untuk mengamankan berkas pada saat pengiriman dengan jaringan internet, sehingga hanya yang memiliki hak akses yang mengetahui isi dari berkas tersebut. Dengan sistem penyimpanan yang dibuat diharapkan pengguna merasa aman dalam mengirim berkas secara online yang menjaga kerahasian dokumen yang dikirimkan[5]

II. METODOLOGI PENELITIAN

A. *Blok Diagram Sistem*

Berikut merupakan Blok diagram sistem yang digunakan untuk sistem penyimpanan data menggunkan *cloud computing* sebagai *Software As A Service* dengan *advanced encryption standard,*

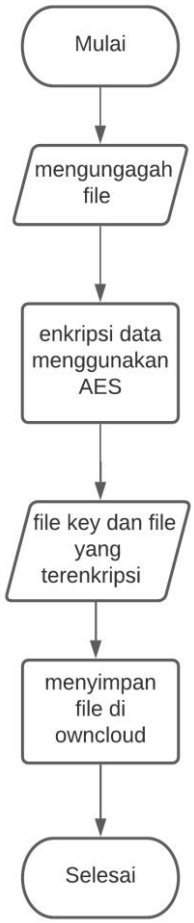


Gambar 1 Blok Diagram sistem

Gambar 1 penjelasan mengenai cara kerja dari sistem ini yaitu Sistem penyimpanan data *cloud computing* yang akan dibuat menerapkan enkripsi *Advanced Encription Standard* (AES) dengan *software OwnCloud. Client* dapat menyimpan data ke *ownCloud* dengan aman dapat menampilkan data, mengubah data dan menghapus data. *Client* dapat mengirim data ke server *cloud* tanpa perlu khawatir data yang akan dikirim dapat dilihat ataupun diambil oleh pihak yang tidak berwenang.

B. *Flowchart Tahapan Sistem*

Berikut merupakan *flowchart* pada sistem Sistem Penyimpanan Data Menggunkan *Cloud computing* Sebagai *Software As A Service* dengan *Advanced Encryption Standard,* terdapat pada gambar 2



Gambar 2 *Flowchart* tahapan sistem

Gambar 2 menjelaskan bahwa Pertama mulai mengunggah file dengan menambahkan file ke dalam system penyimpanan nya atau *ownCloud*. Lalu data dienkripsi dengan menggunakan algoritma Advanced Encryption Standard. Lalu file dicek system agar file key terenkripsi dan apabila memiliki kases dapat terdeskripsi Kembali atau file dapat dibaca. Kemudian data sudah dienkripsi data akan disimpan ke *ownCloud*. Yang tidak memiliki hak akses jika ingin mencuri file tersebut maka file yang diunduh akan bisa dibuka atau menampilkan bahwa file sudah terenkripsi dengan AES.

III. HASIL DAN PEMBAHASAN

A. Implementasi User Interface

Tampilan login ownCloud yaitu halaman untuk mengakses akun yang sudah dibuat dengan login ke akun admin dengan memakai jaringan virtual private server yang sudah disetting sebelumnya. Dapat dilihat pada gambar 3

Gambar 3 Tampilan *login ownCloud*

Gambar 3 Tampilan *login ownCloud* terdapat dua kolom yaitu untuk melakukan login admin atau user yang sudah ditambahkan. Dengan memasukkan username admin yaitu "Nisha" dan password yang sudah dibuat. Kemudian admin akan secara otomatis masuk ke sistem penyimpanan tersebut dan dapat menyimpan file secara online dimanapun.

1. Membuat Instances

Sistem operasi pada vultr dengan membuat instances pada vultr, proses pembuatan instances tersebut menginstall sistem operasi *file iso template* OS Ubuntu 18.04. Hal yang pertama mendeploy server baru dengan tipe cloud compute, lokasi server yang diplih yaitu singapura, sistem operasi yang dipakai yaitu ubuntu 18.04 x64.dan memilih ukuran server dengan spesifikasi CPU:1 vCore, RAM:1024 MB, Storage : 25 GB SSD, Bandwidth : 0.48 GB of 1000 GB. Tampilan instances ada pada gambar 4

Gambar 4 Tampilan instances server pada vultr

2. Konfigurasi web server

Web server digunakan sebagai perangkat lunak yang bertugas untuk menangani permintaan dari *web browser client* dengan mengirimkan *respons* kepada client. *Web server* memerlukan beberapa paket agar dapat berjalan yaitu Apache2 dan PHP. Instalasi paket pendukung web server menggunakan perintah apt install yang dijalankan pada terminal linux ubuntu. Instalasi paket tersebut dapat dilihat pada gambar 5.

```
root@nisha:~# apt install apache2 libapache2-mod-php7.2 openssl php-imagick php7
.2-common php7.2-curl php7.2-gd php7.2-imap php7.2-intl php7.2-json php7.2-ldap
php7.2-mbstring php7.2-mysql php7.2-pgsql php-smbclient php-ssh2 php7.2-sqlite3
php7.2-xml php7.2-zip
Reading package lists... Done
Building dependency tree
Reading state information... Done
php-imagick is already the newest version (3.4.4+php8.0+3.4.4-7+ubuntu20.04.1+de
b.sury.org+1).
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libavahi-client3 libavahi-common-data
  libavahi-common3 libc-client2007e libcups2 libldb2 libpcre3 libpq5
  libsmbclient libssh2-1 libtalloc2 libtevent0 libwbclient0 mlock php7.2-cli
  php7.2-opcache php7.2-readline php8.0-smbclient php8.0-ssh2 python3-talloc
  samba-libs
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
  php-pear uw-mailutils cups-common
Recommended packages:
  ssl-cert
The following NEW packages will be installed:
```

Gambar 5 instalasi web server

3. Pembuatan Database MySQL dan instalasi ownCloud

MySQL adalah sistem manajemen basis data (DBMS) open-source yang sangat populer. DBMS adalah perangkat lunak yang digunakan untuk menyimpan, mengelola, dan mengakses data dalam basis data. MySQL terutama digunakan untuk menyimpan data terstruktur, seperti data dalam bentuk tabel yang terhubung satu sama lain. Berikut tampilan MySQL sudah terpasang pada *database server* dapat dilihat pada gambar 6.

```
root@nisha:~# systemctl status mysql
● mariadb.service - MariaDB 10.3.29 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service
     Active: active (running) since Tue 2021-07-06 08:47
       Docs: man:mysqld(8)
             https://mariadb.com/kb/en/library/systemd/
      Tasks: 33 (limit: 1072)
     Memory: 85.1M
     CGroup: /system.slice/mysql.service
             ├─737 /bin/sh /usr/bin/mysqld_safe
             ├─870 /usr/sbin/mysqld --basedir=/usr --dat
             └─871 logger -t mysqld -p daemon error
```

Gambar 6 *status database MySQL*

Gambar 6 menunjukkan bahwa layanan MySQL telah berjalan di server dengan status *active (running)* dan siap digunakan untuk *ownCloud*. kemudian penginstalan *ownCloud* dengan menggunakan wget https://download.*ownCloud*.org/community/*ownCloud*-10.0.10.zip -P /tmp yang merupakan arsip zip dari *ownCloud*. Proses mengunduh arsip zip pada gambar 7.

```
root@nisha:~# wget https://download.owncloud.org/community/owncloud-10.0.10.zip
-P /tmp
--2021-07-25 09:51:01--  https://download.owncloud.org/community/owncloud-10.0.1
0.zip
Resolving download.owncloud.org (download.owncloud.org)... 167.233.14.167, 2a01:
4f8:1c1d:3d1::1
Connecting to download.owncloud.org (download.owncloud.org)|167.233.14.167|:443.
.. connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://attic.owncloud.org/community/owncloud-10.0.10.zip [following]
--2021-07-25 09:51:02--  https://attic.owncloud.org/community/owncloud-10.0.10.z
ip
Resolving attic.owncloud.org (attic.owncloud.org)... 195.201.36.192, 2a01:4f8:c2
c:5c1d::1
Connecting to attic.owncloud.org (attic.owncloud.org)|195.201.36.192|:443... con
nected.
HTTP request sent, awaiting response... 200 OK
Length: 56865374 (54M) [application/zip]
Saving to: '/tmp/owncloud-10.0.10.zip'

owncloud-10.0.10.zi  90%[=================>  ]  49.13M  10.1MB/s    eta 2s
```

Gambar 7 Mengunduh arsip zip *ownCloud*

Setelah arsip ownCloud berhasil diunduh melalui proses pada gambar 4.10, kemudian dilakukan ekstrak arsip ke direktori "/var/www" yang merupakan direktori utama web

server Apache. Untuk mengekstrak semua file dari arsip ZIP yang telah diunduh, digunakan perintah pada gambar 8 berikut.

```
root@nisha:~# unzip /tmp/owncloud-10.0.10.zip -d /var/www
```

Gambar 8 ekstrak arsip ke direktori

Dengan mengekstrak semua file dari arsip zip maka pada direktori var/www akan terbuat sebuah direktori dengan nama *ownCloud*. Direktori tersebut harus diubah kepemilikannya menjadi www-data. Perintah untuk merubah kepemilikan yaitu menggunakan chown –R, seperti pada gambar 9 berikut.

```
root@nisha:~# chown -R www-data: /var/www/owncloud
```

Gambar 9 Merubah kepemilikan direktori ownCloud.

4. Konfigurasi Virtual Host

Virtual host dikonfigurasi agar direktori *ownCloud* dapat diakses melalui domain utama tanpa harus mendefinisikan letak direktori pada saat pengaksesan di web browser. Konfigurasi virtual host untuk *ownCloud* dilakukan pada file *ownCloud*.conf dan diakses menggunakan perintah "nano /etc/apache2/conf-available/*ownCloud*.conf". file *ownCloud*.conf dikonfigurasi dengan script seperti pada gambar 10 berikut.

```
  GNU nano 4.8        /etc/apache2/conf-available/owncloud.conf
Alias / "/var/www/owncloud/"

<Directory /var/www/owncloud/>
  Options +FollowSymlinks
  AllowOverride All

 <IfModule mod_dav.c>
  Dav off
 </IfModule>

 SetEnv HOME /var/www/owncloud
 SetEnv HTTP_HOME /var/www/owncloud

</Directory>
```

Gambar 10 Konfigurasi virtual host

Gambar 10 dapat dijelaskan bahwa direktori root (/) diarahkan ke direktori "/var/www/*ownCloud*/" sehingga saat diakses melalui browser akan otomatis diarahkan ke direktori instalasi *ownCloud*. Agar virtual host yang dikonfigurasi tersebut aktif, dilakukan pengaktifan konfigurasi yang baru ditambahkan dan semua modul Apache yang diperlukan dengan perintah seperti pada gambar 11 berikut.

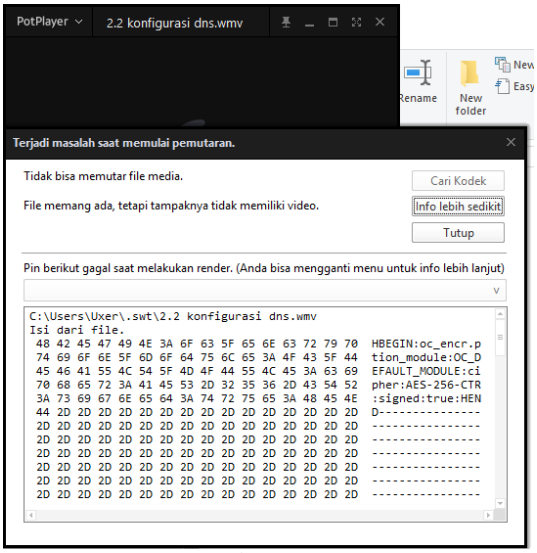
```
root@nisha:~# a2enconf owncloud
Enabling conf owncloud.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@nisha:~# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@nisha:~# a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@nisha:~# a2enmod env
Module env already enabled
(reverse-i-search)`': a2enmod di^C
root@nisha:~# a2enmod dir
Module dir already enabled
root@nisha:~# a2enmod mime
Module mime already enabled
```

Gambar 11 Mengaktifkan Konfigurasi Apache

B. Pengujian Sistem

1. Pengujian keamanan data yang ada di ownCloud

Pengujian keamanan data di *ownCloud* dengan menerapkan algoritma AES dilakukan dengan menggunakan aplikasi filezilla untuk dapat mengecek apakah data yang diunduh melalui filezilla dapat terbaca, pengujian awal dengan mengunduh video yang ada di *ownCloud*. Berikut hasil pengujian terhadap file video yang ada di *ownCloud* dengan mengunduhnya di aplikasi filezilla *seperti pada gambar 12.*

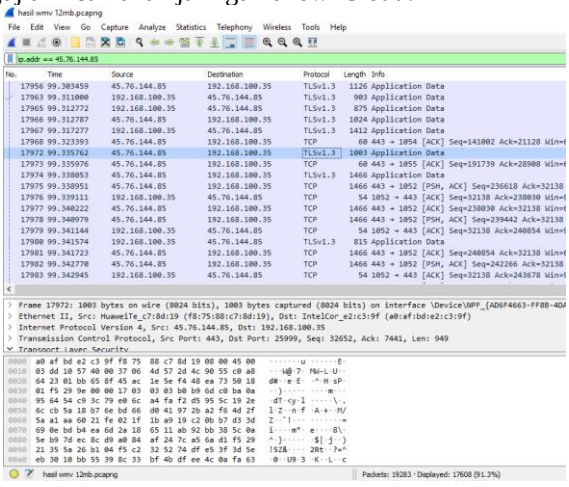


Gambar 12 Hasil file yang terenkripsi AES

Gambar 12 adalah Hasil yang didapat yaitu video tidak dapat terbaca karena *ownCloud* memiliki keamanan enkripsi AES yang data tersebut tidak bisa dicuri dengan mudah oleh seorang hacker, bahkan admin dan pengguna yang lain tidak dapat mengambilnya. Karena data yang ada di *ownCloud* sudah terenkripsi oleh AES 256 yang berada didalam host namun tidak bisa dibaca karena sudah terenkripsi.

2. Pengujian *Keamanan Koneksi Klien Server*

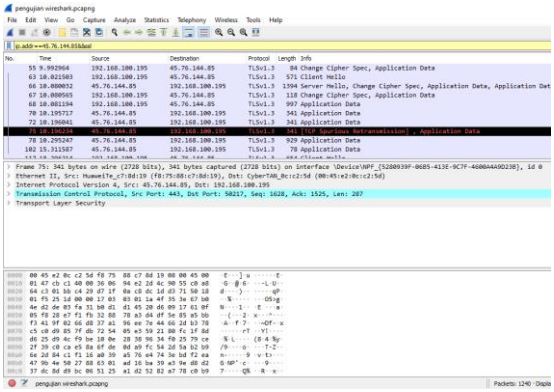
Pengujian keamanan jaringan pada website dilakukan untuk mengetahui koneksi antara klien dan server *ownCloud* sudah terenkripsi dengan benar atau tidak. Berikut hasil pengujian keamanan jaringan di *ownCloud*.



Gambar 13 *hasil penyaringan paket data Nisha.my.id*

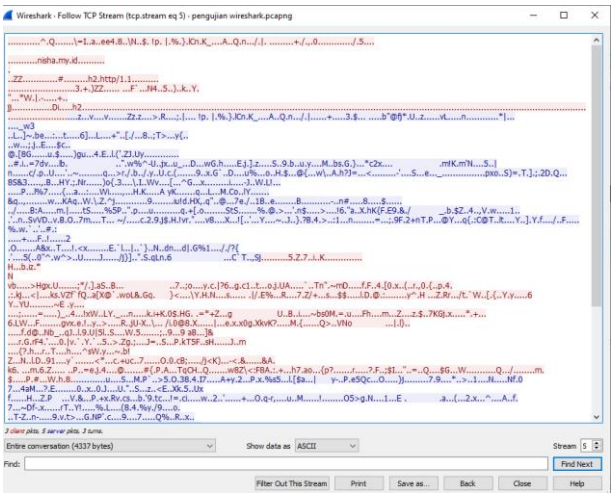
Gambar 13 ialah seluruh paket data yang memiliki IP Address 45.76.144.85 yang ada pada Source dan pada Destination. Antara Source dan Destination yang sering menukar tempat. Dari 17608 paket data yang ada terdapat 2 jenis *protocol* yang dipakai yaitu *transmission control protocol* (TCP) dan *transport layer security* (TLS).

Kemudian menganalisa keamanan pada website apakah terenkripsi dengan benar, maka dilakukan penyaringan lagi dengan mengetik perintah "ip.addr==45.76.144.85&&ssl" maka akan tampil paket-paket yang ada terdapat pada pada gambar 14 berikut.



Gambar 14 Paket Data Nisha.my.id dengan Protokol TLS

Pada Gambar 14 merupakan paket data pada website Nisha.my.id yang memiliki protokol TLS. Pada menu info memiliki keterangan-keterangan seperti Server Hello, Server Key Exchange, Certificate, Client Key Exchange, Clint Hello, Application Data dan Change Cipher Spec. Untuk analisis paket dapat dikerjakan dengan cara klik kanan pada paket data yang ingin dilakukan analisis kemudian klik Follow SSL Stream. Berikut ialah suatu tampilan detail packet data *protocol* TLS yang memiliki info aplikasi Data. Paket data pada Application data ada pada gambar 15.



Gambar 15 Follow Tcp Stream

Gambar 15 yaitu tampilan dari gambar Follow TCP Stream dari data yang diklik atau dipilih sebelumnya. Dari detail paket data *protocol* TLS yang dilakukan pada gambar 15 tidak ditemukan data atau infomasi apapun. Dapat dianalisis pada paket data dengan cara mengklik kanan pada paket data yang ingin dianalisa kemudian klik Follow TCP Stream. Berdasarkan info Follow TCP Stream, dianalisis bahwa data tidak dapat dianalisa informasinya. Hal tersebut dikarenakan bahwa data yang dikirim telah terenkripsi sehingga data tidak dapat dibaca.

IV. KESIMPULAN

Adapun berdasarkan pembahasan dan pengujian yang telah dilakukan pada sistem Sistem Penyimpanan Data Menggunakan Cloud computing sebagai Software-as- a-Service dengan Advanced Encryption Standard, dapat disimpulkan sebagai berikut.

1. Dari hasil uji mengakses data secara langsung menggunakan filezilla, file yang diunggah melalui ownCloud telah terenkripsi menggunakan algoritma AES yang dibuktikan dengan hasil yaitu isi file yang diakses secara langsung dalam bentuk chipertext.
2. Pengujian menggunakan wireshark mendapatkan hasil yaitu lalu lintas data pada jaringan hanya menampilkan data dalam bentuk chipertext. Sehingga koneksi antara klien dan server telah berhasil dienkripsi menggunakan TLS.

REFERENSI

[1] A. (2014). Studi Perbandingan Layanan Cloud Computing. *Jurnal Rekayasa Elektrika*, *10*(4). https://doi.org/10.17529/jre.v10i4.1110

[2] Susanto, W. E. (2014). Pendekatan Keamanan Serta Kecepatan Akses Data Pada Cloud. Bianglala Informatika, 2(2), 79–87.

[3] Dedi Kurniawan, Rita Afyenni, R. H. (2018). Implementasi Algoritma AES dalam Mengenkripsi Berkas Terintegrasi dengan Layanan Cloud Storage Berbasis Android. ISSN Media Elektronik, 3(September), 4–5.

[4] Indrayani, L. A., & Suartana, I. M. (2019). Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document. Jinacs, 01(1), 42–47.

[5] Imamah, Djunaidy, A., & Husni, M. (2014). Penerapan AES Untuk Otentikasi Akses Cloud Computing. Ilmiah SimanteC, 4(1), 3–5. http://www.ncbi.nlm.nih.gov/pubmed/22352137