Implementasi *Secure Storage* Menggunakan *Metode Full Disk Encryption* dan *Tamper Proof* pada *Cloud Storage*

Barok Rizqi[1)], Andriani Adi Lestari[2)]
(1) Badan Siber dan Sandi Negara, barok.rizqi@bssn.go.id
(2) Badan Siber dan Sandi Negara, andriani.adi@bssn.go.id

Abstrak

Saat ini pengembangan storage telah berubah menjadi penyimpanan berbasis internet atau yang dikenal dengan cloud storage sebagai media penyimpanan dalam jaringan. Cloud storage lebih banyak diminati oleh masyarakat umum karena memiliki beberapa kelebihan, di antaranya ketika penyimpanan pada personal komputer habis, pengguna tidak perlu membeli perangkat penyimpanan baru ataupun mengeluarkan biaya tambahan untuk pemeliharaan perangkat. Namun penggunaan penyimpanan berbasis online tersebut dapat meningkatkan risiko seperti akses tidak sah, kebocoran data, informasi sensitif, dan hak privasi. Pada penelitian ini diusulkan sebuah prototipe secure personal cloud storage dengan pelindungan fisik pada pangkalan data. Perangkat yang dibangun memiliki fitur enkripsi data menggunakan metode full disk encryption untuk mengamankan data pada peladen, Virtual Privat Network (VPN) untuk mengamankan komunikasi antara user-server, dan tamper proof untuk mengamankan database secara fisik. Hasilpengujian menunjukkan bahwa implementasi secure storage mempengaruhi performa dari cloud storage, dibuktikan dengan adanya penurunan kecepatan write data dari 19,87 Mb/s menjadi 15,75 Mb/s setelah diterapkan Linux Unified Key Setup (LUKS) full disk encryption. Pada sisi keamanan transmisi data, OpenVPN dapat mengamankan tansmisi antara user dan server. Hal ini dibuktikan dengan pengujian sniffing menggunakan tools wireshark yang menunjukkan bahwa pengiriman data telah dienkapsulasi oleh aplikasi OpenVPN. Pada unit testing yangdilakukan pada LUKS, membuktikan bahwa jumlah key slot LUKS versi 2 maksimal 32 key slot. Pengujian yang terakhir membuktikan bahwa mekanisme tamper proof dapat bekerja sesuai harapan. Mekanisme tamper proof bekerja ketika perangkat mendeteksi adanya indikasi serangan pada perangkat fisik. Pengujian yang dilakukan yaitu melakukan perusakan pada casing perangkat menggunakan palu, membuka baut casing, dan gergaji. Hasil pengujian menunjukkan bahwa perangkat akan menjalankan perusakan pada SSD ketika indikasi serangan melebihi nilai toleransi.

Kata kunci: cloud storage (1), LUKS full disk encryption (2), storage (3), VPN (4)

Abstract

Currently, storage development has shifted to internet-based storage, or cloud storage, as online storage media. Cloud storage is becoming more popular among the public due to several advantages, including the fact that when the storage on personal computers runs out, users do not need to purchase new storage devices or incur additional costs for device maintenance. However, using such online storage can increase risks such as unauthorized access, data leakage, sensitive data, and privacy rights. This study proposes a prototype secure personal cloud storage system with physical database protection. The device has data encryption features that use full disk encryption to secure data on the server, VPN to secure communication between user and server, and tamper proof to physically secure the database. The test results show that the implementation of secure storage affects the performance of cloud storage, as evidenced by the decrease in data write speed from 19.87 Mb/s to 15.75 Mb/s after the implementation of LUKS full disk encryption. On the security side of data transmission, OpenVPN can secure the transmission between the user and the server. This is evidencedby sniffing testing using wireshark tools which shows that data transmission has been encapsulated by the OpenVPN application. In unit testing carried out on LUKS, it proved that the number of LUKS version 2 key slotscorresponds to the reference, which is a maximum of 32 key slots. The last test proves that the tamper proof mechanism can work as expected. The tamper proof mechanism works when the device detects an indication of anattack on the physical device. The tests carried out were destroying the device casing using a hammer, opening the casing bolt, and a saw. The test results show that the device will perform damage to the SSD when the attack indication exceeds the tolerance value.

Keywords: cloud storage (1), LUKS full disk encryption (2), storage (3), VPN (4)

.

1. PENDAHULUAN

Saat ini, kebutuhan penyimpanan data semakin meningkat. Untuk itu diperlukan media penyimpanan berkapasitas besar yang dapat digunakan untuk menyimpan berbagai jenis data. Tidak hanya berkapasitas besar, fleksibilitas dan keamanan data juga menjadi aspek yang patut diperhatikan dalam sebuah media penyimpanan. Pada era digital ini, *storage* telah berkembang menjadi penyimpanan berbasis internet atau yang dikenal dengan *cloud storage* sebagai media penyimpanan *online*. Sebelum maraknya penggunakaan *cloud storage*, masyarakat menggunakan local *storage* untuk menyimpan data. Namun keterbatasan kapasitas dan fleksibilitas yang dimiliki *local storage* sehingga *cloud storage* kini lebih banyak diminati. Hal ini dikarenakan pengguna tidak perlu mengeluarkan biaya tambahan untuk pemeliharaan perangkat. Selain itu could storage juga dinilai lebih unggul jika dibandingkan dengan *local storage* karena dapat diakses di mana saja dan dengan perangkat apa saja [1].

Terdapat banyak kelebihan pada penyimpanan berbasis online. Selain memiliki banyak kelebihan, penyimpanan berbasis *online* juga dapat meningkatkan risiko seperti akses tidak sah, kebocoran data, informasi sensitif, dan hak privasi[2]. Oleh karena itu, penyimpanan berbasis online harus didukung dengan layanan keamanan agar aman terhadap berbagai kerawanan, khususnya penyimpanan berbasis online yang digunakan oleh instansi pemerintah karena terdapat instansi pemerintah yang mengelola informasi bersifat terbatas[2].

Terdapat beberapa penelitian yang telah dilakukan tentang *cloud storage*. Seperti pada penelitian [3] yang berhasil membangun sebuah *prototype* raspberry Pi personal *clouds storage* yang dikelola secara personal/pribadi. Namun pada penelitian tersebut belum diterapkan keamanan berupa enkripsi data atau keamanan fisik.

Pada tahun 2019, Faizianur [2] berhasil membuat *Secure Data Sharing in Clouds* (SeDaSC) dengan mengenkripsi database menggunakan AES-256 pada sisi *client*. Aplikasi berbasis web tersebut dibangun menggunakan API dari google drive. Sistem *cloud* yang dibangun dapat digunakan secara bersama dengan pengguna lain dan dibangun dengan asumsi komunikasi pengguna dan server aman.

Berdasarkan latar belakang diatas, maka pada penelitian ini diusulkan sebuah secure personal *cloud storage* dengan pelindungan fisik pada *database*. Perangkat yang akan dibangun memiliki fitur enkripsi data menggunakan metode *full disk encryption* pada sisi server untuk mengamankan data pada server, VPN untuk mengamankan komunikasi antara user dan server, dan *tamper proof* untuk mengamankan *database* secara fisik.

Metode *full disk encryption* bekerja dengan melakukan *enkripsi storage* pada perangkat penyimpanan. Apabila pengguna tidak memiliki passphrase maka data pada disk tersebut tidak dapat diakses. Passphrase pada LUKS digunakan sebagai material kunci untuk melakukan enkripsi dan dekripsi. LUKS yang akan diterapkan mempunyai 32 key slot, passphrase disimpan pada key slot [4]. Linux Unified Key Setup (LUKS) memiliki beberapa algoritme yang dapat diterapkan. Pada penelitian akan digunakan algoritme AES-256 sebagai algoritme enkripsi dan dekripsi pada LUKS full disk encryption. Pada sisi keamanan transmisi data, VPN yang digunakan yaitu OpenVPN Server berbasis opensource. Tamper proof yang digunakan pada penelitian ini menggunakan mekanisme *tamper detection* berupa penghancuran alat. Penghancuran yang dilakukan sesuai dengan physical security requirements for cryptographic modules pada standar SNI ISO/IEC 19790 [5]. Mekanisme penghancuran alat dipilih karena merupakan mekanisme terbaik dan termudah untuk dilakukan [6].

2. LANDASAN TEORI

Bagian ini membahas studi literatur yang berkaitan dengan penelitian yang dilakukan, diantaranya Cloud Storage, Linux Unified key Setup, Tamper Proof, dan Virtual Private Network.

2.1. Cloud Storage

Cloud storage atau penyimpanan awan adalah salah satu pengembangan dari teknologi cloud computing[7][8], [9]. Cloud storage dapat digunakan untuk menyimpan data, back up data, dan mengolah data pada resource yang telah disediakan. Penyedia layanan cloud storage menyediakan layanan sebagai pengolah resource, selain itu pengguna juga dimudahkan untuk berbagi data dengan pengguna lainnya [2]. Struktur dari cloud storage terbagi menjadi 4 layer:

a. Storage layer

Lapisan ini merupakan lapisan paling dasar dari cloud storage. Sistem penyimpanan cloud storage terdiri dari banyak perangkat penyimpanan yang terdistribusi di berbagai wilayah yang terhubung melalui jaringan internet, atau fiber channel. [10].

b. Management layer

Lapisan manajemen merupakan sebuah inti dari cloud storage, lapisan manajemen ini mengolah beberapa perangkat penyimpanan di cloud storage melalui perangkat fisik penyimpanan berupa cluster [10].

c. Application interface layer

Lapisan ini merupakan bagian paling fleksibel dari cloud storage. Pengelola layanan cloud storage memiliki tampilan antarmuka yang berbeda dalam

penyedia layanannya. Misalnya remote backup data application platform, network hard disk application platform, IPTV dan video-on-demand (VOD) [11].

d. Access layer

Pada bagian ini dilakukan manajemen user sesuai rules yang diberlakukan oleh penyedia provider, setiap user yang berwenang dapat melakukan akses layanan pada sistem penyimpanan cloud storage [11].

Saat ini sudah banyak layanan cloud storage yang tersedia dari yang bersifat gratis hingga berbayar dengan berbagai fasilitas termasuk jaminan keamanan terhadap data pengguna[2]

2.2. Linux Unified Key Setup

Penyimpanan data dalam bentuk memory USB saat ini sering digunakan sebagai proses perpindahan informasi ataupun penyimpanan perlindungan data sensitif. Karena perangkat tersebut merupakan yang paling umum digunakan karena kemudahannya. Penyimpanan yang digunakan cenderung menyimpan informasi yang sensitif dan tidak dilindungi dan jika perangkat tersebut hilang atau dicuri tentunya terdapat pihak yang akan dirugikan jika data sensitif tersebut hilang dan dimanfaatkan untuk tindakan kejahatan[4]. Pada tahun 2004 dikenalkan sebuah teknologi oleh linux yang dapat memberikan layanan keamanan pada sebuah perangkat seperti secure digital (SD) card, flash disk, harddisk, ataupun solid state drive (SSD). Teknologi tersebut yaitu Linux Unified Key Setup (LUKS)[12].

LUKS diimplementasikan untuk melakukan full disk encryption pada perangkat storage yang digunakan [4]. Pada perangkat yang dibangun oleh [6], LUKS diimplementasikan untuk mengamankan sebuah SD card dari perangkat manajemen kunci yang dibangun. LUKS merupakan standar untuk enkripsi hard disk pada sistem operasi linux yang menggunakan skema TKS1. Skema tersebut merupakan skema key setup yang memiliki fitur anti forensic dan two-level encryption. LUKS memiliki 4 perintah high-level yang dapat dijalankan, yaitu create partition, open partition, add key, dan revoke key.

2.3. Tamper Proof

Tamper proof merupakan mekanisme perlindungan secara otomatis pada perangkat kriptografi terhadap adanya upaya yang dilakukan sehingga dapat membahayakan perangkat tersebut [6]. Tamper proof digunakan untuk mencegah terjadinya gangguan dan kemungkinan intrusi pada lapisan fisik pada perangkat kriptografi. Terdapat beberapa jenis mekanisme yang cukup popular dan banyak digunakan seperti destroying, send notification, dan turn on physical indicator. Pada penelitian [6] dilakukan penghancuran alat karena merupakan mekanisme yang terbaik dan mudah diterapkan. Metode penghancuran yang digunakan dapat merusak alat menggunakan tegangan yang melebihi batas toleransi pada perangkat. Dampak yang ditimbulkan dari hal tersebut yaitu rusaknya media penyimpanan yang berisikan segala informasi atau data sensitive pada perangkat yang dibangun[13], [14].

2.4. Virtual Private Network

Virtual Private Network adalah seperangkat alat yang memungkinkan jaringan di lokasi berbeda untuk dapat saling terhubung dengan aman, menggunakan jaringan *public* sebagai lapisan transport[15]. VPN banyak digunakan oleh suatu organisasi atau perusahaan dalam menyediakan akses jaringan internalnya kepada pihak luar [16]. Terdapat beberapa layanan yang menyediakan protokol OpenVPN, yang mudah untuk diterapkan salah satunya yaitu tools OpenVPN server pada raspberry pi. Pada penelitian yang akan dilakukan, digunakan OpenVPN. Proses pembangkitan sertifikat menggunakan Easy-RSA. Easy-RSA adalah tools manajemen infrastruktur kunci publik yang digunakan pada server OpenVPN[17].

3. METODE PENELITIAN

Dalam perancangan dan pembangunan penelitian ini akan diterapkan metodologi penelitian menggunakan metode Sistem Development Life Cycle (SDLC) dengan pendekatan yang dipilih yaitu waterfall. Pada proses pembangunan sistem menggunakan pendekatan waterfall yang memiliki 4 tahap berupa planning (perencanaan), analysis (analisis), design (desain), dan implementation (implementasi)[18].

a. Perencanaan

Proses yang dilakukan pada tahap ini adalah studi literatur dan konsultasi. Studi literatur digunakan untuk menentukan ruang lingkup pengembangan, masalah apa saja yang dapat diselesaikan, menentukan dan mengevaluasi strategi yang digunakan dalam mengembangkan system

b. Analisis

Tujuan dari tahap ini adalah untuk menentukan kebutuhan dari sistem yang dibangun. Hasil tahap ini berupa kebutuhan fungsional, kebutuhan non fungsional, kebutuhan software, dan kebutuhan hardware

c. Perancangan

Perancangan sistem merupakan tahap penentuan mengenai bagaimana sistem akan beroperasi, perangkat yang yang akan digunakan untuk mengoperasikan sistem, interface pengguna dan segala hal yang dibutuhkan dalam membangun sistem. Pada tahap ini digambarkan bagaimana sistem bekerja.

d. Implementasi

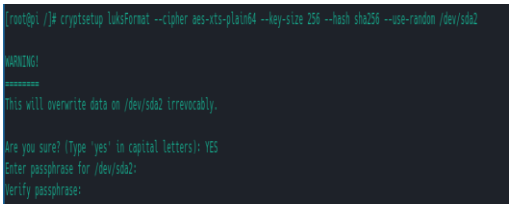
Hasil dari tahap desain yang telah dirancang selanjutnya diimplementasikan pada komponen software dan hardware yang telah ditentukan. Adapun hal yang akan diimplementasikan adalah raspberry pi 4 menjalankan sistem operasi Manjaro ARM64 sebagai cloud server, karena sistem operasi pada raspberry yang mendukung untuk menerapkan metode full disk encryption saat ini adalah Manjaro ARM64 untuk menerapkan sistem keamanan pada penyimpanan berupa enkripsi pada storage menggunakan LUKS full disk encryption. Untuk keamanan fisik dari database, akan diterapkan mekanisme tamper proof menggunakan sensor getar. Terdapat beberapa pengujian setelah dilakukannya implementasi. Pengujian dilakukan untuk mengetahui bahwa implementasi yang dilakukan sesuai dengan harapan.

4. HASIL DAN PEMBAHASAN

Pada bagian ini dibahas mengenai implementasi dan hasil pengujian yang dilakukan pada perangkat yang telah dibangun.

a. Implementasi Registrasi Passphrase

Setelah melakukan instalasi LUKS pada Raspberry Pi 4, tahap ini merupakan proses Admin untuk melakukan pendaftaran passphrase LUKS ditunjukkan pada Gambar 1. Passphrase tersebut disimpan pada SSD, dan nantinya digunakan sebagai parameter material kunci untuk algoritme PBKDF2 dan AES-256. Pada proses booting nantinya passphrase tersebut digunakan admin untuk dapat melakukan akses pada sistem operasi dari cloud server, sehingga admin dapat mengelola cloud server.



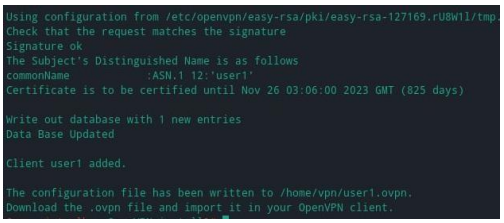
Gambar 1 Pendaftaran *Passphrase*

b. Implementasi Pembangkitan Sertifikat VPN User

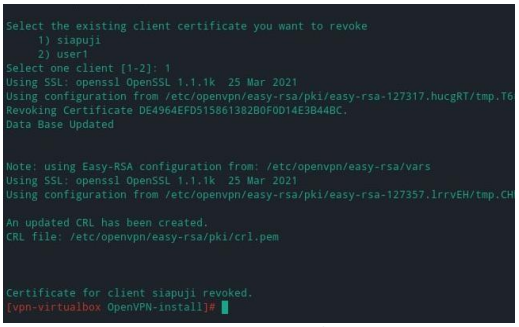
Proses ini dilakukan setelah instalasi OpenVPN. Pembangkitan sertifikat VPN untuk user dilakukan oleh admin dengan melakukan input data user berupa username, dan password user. Algoritme yang dipilih yaitu RSA 2048. Sertifikat yang dibangkitkan memiliki masa berlaku selama 825 hari. Setelah proses pembangkitan sertifikat selesai, maka akan tampil seperti pada Gambar 2. Sertifikat tersebut akan diberikan kepada user secara offline dan dapat langsung digunakan pada aplikasi OpenVPN.

c. Implementasi Revoke Sertifikat VPN User

Untuk melakukan revoke sertifikat, admin membuka konsol OpenVPN server, dan memilih menu Revoke exiting user. Setelah memilih menu tersebut, maka akan muncul list user yang telah terdaftar sebelumnya dan admin dapat langsung melakukan revoke sertifikat user yang dipilih, ditunjukkan pada Gambar 3. Sertifikat user yang telah dihapus, tidak dapat terhubung kembali ke server VPN.



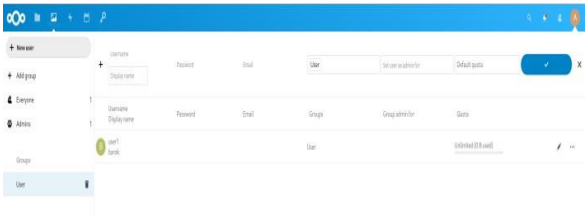
Gambar 2 Pembangkitan Sertifikat VPN User



Gambar 3 Penghapusan Sertifikat VPN User

d.* Implementasi *Add User Cloud

Setelah dilakukan pembangunan infrastruktur pada koneksi jaringan berupa VPN, adminmelakukan penambahan *user*. Penambahan *user* memerlukan identitas dari *user* yaitu *username* dan *password*. Pada proses pendaftaran *user*, *admin* juga melakukan manajemen untuk *user* agarmendapatkan hak untuk melakukan *upload* dan *download* serta batas maksimal penyimpanan yang dimiliki. Hasil dari penambahan *user* ditunjukkan pada Gambar . Setelah *admin* berhasil menambahkan *user* baru, *user* diharuskan untuk mengganti *password* pada akun yang telah diberikan. Apabila *user* lupa *password* akun tersebut, *user* dapat menghubungi *admin* dan meminta untuk menonaktifkan akun tersebut atau meminta melakukan *reset password*.

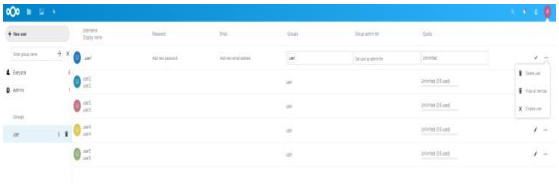


Gambar 4 Menambahkan User Cloud

e.* Implementasi *Remove User Cloud

Pada sistem yang dibangun, *cloud server* tidak dapat mengganti *password* atau tidak terdapat fitur

"*forgot password?*", sehingga user harus menghubungi admin untuk melakukan *reset password* atau meminta menonaktifkan akun tersebut. Hasil dari implementasi fitur tetersebut ditunjukkan pada Gambar 5 .



Gambar 5 Menghapus User Cloud

f. Implementasi Menghubungkan pada *Server* VPN

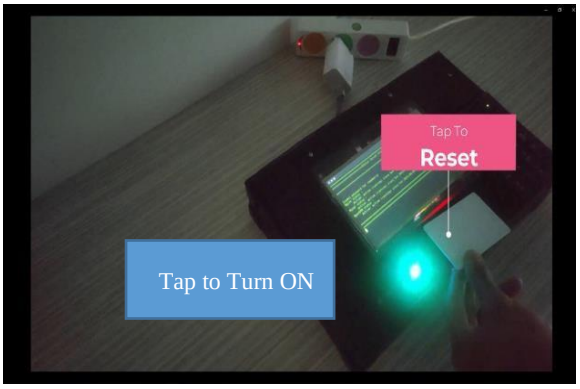
Setelah *user* mendapatkan sertifikat VPN dari *admin*, *user* dapat menggunakan sertifikat tersebut untuk terhubung pada *server* VPN. Apabila sertifikat *user* autentik, maka *user* tersebut akan terhubung pada *server* VPN seperti yang ditunjukkan pada Gambar 6. Setelah *user* terhubung ke *server* VPN, nantinya *user* dapat melakukan akses pada *cloud server* dengan membuka domain dari *cloud server*

g. Implementasi *Login Cloud Server*

Tahap selanjutnya yaitu implementasi *login* pada *cloud* server. Ketika *user* telah terhubung pada VPN server, maka *user* dapat melakukan akses pada *cloud server*. User membuka browser untuk melakukan akses pada alamat domain *http://192.168.0.140/*. Gambar 7 merupakan tampilan awal setelah *user* membuka domain tersebut. *User* diminta untuk melakukan *input username* dan *password* yang telah didaftarkan.

Gambar 6 Koneksi ke server VPN

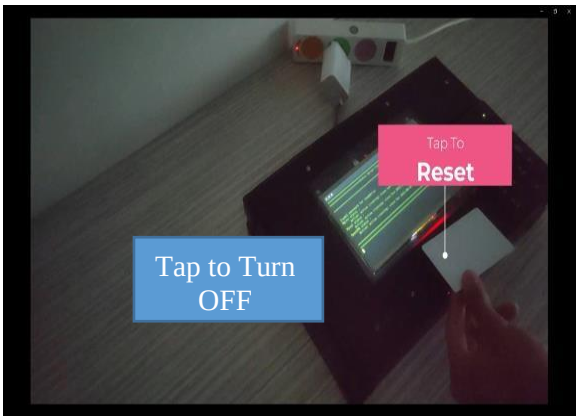
Gambar 7 Tampilan Login Cloud Server



Gambar 8 Menyalakan Tamper Proof

h. Implementasi *Turn On* dan *Turn Off Tamper Proof*

Implementasi yang terakhir yaitu *turn on* dan *turn off* pada mekanisme *tamper proof*. Fungsi ini digunakan untuk mencegah terjadinya kerusakan apabila perangkat tersebut dipindahkan atau terdapat getaran yang dapat dideteksi oleh perangkat, sehingga *admin* dapat melakukan *turn on* atau *turn off* pada mekanisme *tamper proof* ini. Untuk melakukan *turn on* dan *turn off tamper proof*, *admin* dapat melakukan *tap* RFID *card* pada perangkat. Gambar 8 menunjukkan *admin* melakukan *turn on* pada mekanisme *tamper proof* dan Gambar 9 merupakan *turn off* pada mekanisme *tamper proof*.



Gambar 9 Mematikan Tamper Proof

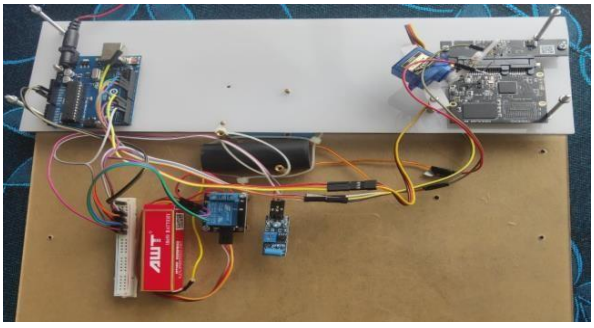
i. Integrasi Komponen Perangkat Keras pada *Server*

Hasil perancangan diimplementaikan dengan menggunakan Raspberry Pi 4, LCD 7 *Inc*, dan SSD sebagai penyimpanannya. Gambar 10 merupakan hasil setelah dirangkai dengan penambahan *keyboard* digunakan sebagai input *passphrase* pada proses *booting* karena telah di implementasikan LUKS pada *cloud server*.

Gambar 10 Integrasi perangkat keras pada server

j. Integrasi Komponen Perangkat Keras pada *Tamper Proof*

Hasil perancangan *tamper proof* di implementasikan menggunakan Arduino UNO, *vibration sensor*, RFID RC522, modul *relay*, motor *servo*, dan *High Voltage Generator*. Gambar 11 merupakan implementasi rangkaian pada *tamper proof* sesuai dengan perancangan yang telah dilakukan. Gambar 12 merupakan penggabungan dari implementasi *server* dan *tamper proof* yang dilakukan pengemasan menggunakan *casing* berbahan akrilik.

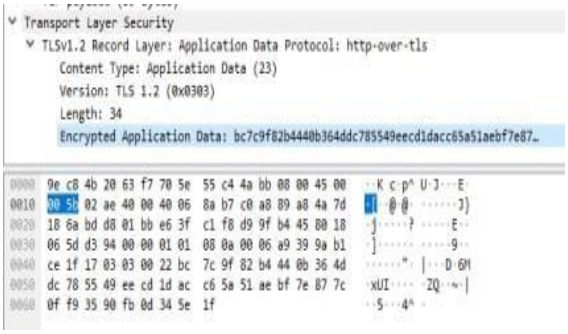


Gambar 11 Rangkaian sensor pada Tamper Proof

Gambar 12 Perangkat Yang Telah di Rangkai

k. **Security Testing**

Security testing dilakukan untuk membuktikan bahwa mekanisme keamanan yang diterapkan bekerja sesuai dengan harapan. Pada *security testing* terdapat dua hal yang perlu diuji, yaitu pada transmisi data dan *tamper proof* pada server sebagaimana ditunjukkan pada Gambar 13.



Gambar 13 Pengujian Keamanan Transmisi Data

a) Keamanan Transmisi Data

Pengujian ini ditujukan untuk mengetahui bahwa keamanan transmisi data dapat dilakukan dengan menerapkan VPN. Pengujian keamanan transmisi data menggunakan 2 skenario yang dilakukan menggunakan *tools wireshark*. Skenario pertama yaitu transmisi *server* yang tidak menggunakan keamanan Tunnel VPN dan skenario kedua yaitu transmisi *server* menggunakan Tunnel VPN. Data yang dirimkan menunjukkan bahwa telah dibungkus (*encapsulated by VPN*) oleh *tunnel* VPN sehingga menampilkan data dalam bentuk terenkripsi dari OpenVPN. Dapat dibuktikan pada pengujian kedua, bahwa VPN dapat melakukan pengamanan pada transmisi data.

b) Keamanan *Tamper Proof*

Pengujian *tamper proof* menggunakan skenario membuka isi perangkat dengan perusakan *casing* perangkat menggunakan beberapa alat. Pada pengujian ini menggunakan *casing* berbahan akrilik 0.5 mm. Terdapat 3 skenario yang dilakukan pada pengujian ini. Skenario pertama dilakukan menggunakan gergaji, skenario kedua menggunakan palu dan pahat, dan untuk skenario ketiga menggunakan obeng untuk membuka skrup penutup pada *casing tamper proof* ditunjukkan pada Table 1. Dari hasil pengujian tersebut menunjukkan respon system dengan hasil indikator merah merupakan indikator sistem melakukan perusakan pada perangkat. Untuk indikator hijau dan kuning merupakan indikator yang menjadi batas toleransi getaran yang diterima.

l. Performace Testing

Pengujian ini dilakukan pada SSD yang telah diterapkan LUKS dan belum diterapkan LUKS.

Pengujian ini dilakukan sebanyak 5 kali pada masing – masing SSD. *Tools* yang digunakan pada Tabel merupakan hasil dari pengujian performa SSD menggunakan *tools ssd benchmark. Tools* tersebut menguji kecepatan rata - rata dalam proses *write data* dengan ukuran 8192 Mb. Dari pengujian tersebut, implementasi dari LUKS mempengaruhi dan menyebabkan penurunan kecepatan pada SSD.

Tabel 1. Indeks Pengujian Getaran

Skenario	Alat	Usaha yang dilakukan	Respon Sistem
Pertama	Gergaji	2 kali gerakan (atasbawah)	Indikator Hijau
		4 kali gerakan (atas bawah)	Indikator Kuning
		6 kali gerakan (atasbawah)	Indikator Merah
Kedua	Palu dan Pahat	4 kali ketukan	Indikator Hijau
		5 kali ketukan	Indikator Kuning
		7 kali ketukan	Indikator Merah
Ketiga	Obeng Membuka Baut	2 Baut terbuka	Indikator Hijau
		3 Baut terbuka	Indikator Kuning
		6 Baut terbuka	Indikator merah

Tabel 2. Kecepatan *Read and Write* pada SSD

Percobaan	*Throughput*			
	SSD 1*		SSD 2**	
	Waktu	Kecepatan	Waktu	Kecepatan
1	8 m 49 s	15.48 Mb/s	6 m 59 s	19.53 Mb/s
2	8 m 29 s	16.09 Mb/s	6 m 59 s	19.55 Mb/s
3	8 m 39 s	15.76 Mb/s	6 m 42 s	20.34 Mb/s
4	8 m 43 s	15.64 Mb/s	6 m 52 s	19.87 Mb/s
5	8 m 38 s	15. 80 Mb/s	6 m 47 s	20.09 Mb/s
Rata rata	8 m 38 s	15.75 Mb/s	6 m 51 s	19.87 Mb/s

*SSD yang telah diterapkan LUKS
**SSD yang belum diterapkan LUKS

5. KESIMPULAN

Setelah dilakukan pengujian dan analisis dari perancangan dan implementasi pada penelitian ini, maka penulis dapat menarik kesimpulan bahwa implementasi *secure storage* mempengaruhi performa dari *cloud storage*, yang ditunjukkan dengan adanya penurunan kecepatan *write data* dari 19,87 Mb/s menjadi 15,75 Mb/s setelah diterapkan LUKS *full disk encryption* pada SSD *cloud storage*. Hal tersebut dikarenakan pada proses *read and write* terdapat proses enkripsi dan dekripsi menggunakan LUKS, lalu padaRaspberry Pi 4 juga terdapat permasalahan pada penggunaan USB 3.0 yang menyebabkan *downspeed*, sehingga pada penelitian ini menggunakan USB 2.0.

Implementasi OpenVPN dapat mengamankan tansmisi antara *user* dan *server*, dibuktikan dengan pengujian *sniffing* menggunakan *tools wireshark*. Dari hasil pengujian menggunakan *wireshark*, data yang dikirimkan oleh *user* terbungkus (*encapsulated by application*), sehingga isi dari data tersebut tidak dapat terlihat oleh penyerang.

Penerapan mekanisme *tamper proof* menggunakan sensor getar dapat mendeteksi adanya indikasi serangan pada perangkat fisik, sehingga mekanisme *tamper proof* yang diusulkan dapat memberikan fitur keamanan fisik pada perangkat personal *cloud storage*. Apabila sensor mendeteksi getaran yang melebihi batas atas nilai toleransi yang ditetapkan, maka perangkat akan melakukan perusakan dengan cara memberikan tegangan melebihi batas maksimal dari perangkat.

REFERENSI

[1] S. Bhalla, P. Kwan, M. Bedekar, R. Phalnikar, · Sumedha, and S. Editors, "Proceeding of International Conference on Computational Science and Applications Algorithms for Intelligent Systems Series Editors: Jagdish Chand Bansal · Kusum Deep · Atulya K. Nagar." [Online]. Available: http://www.springer.com/series/16171

[2] F. Afif, "Rancang Bangun Aplikasi Secure Data Sharing."

[3] Faisal, "RASPBERRY PI PERSONAL

CLOUD STORAGE Major Project," 2015.

[4] M. Brož and M. Broz, "LUKS2 On-Disk Format Specification Version 1.0.0 Document History," 2018.

[5] BSN, "Standar Nasional Indonesia Teknologi informasi-Teknik keamanan-Persyaratan keamanan untuk modul kriptografi," 2012. [Online]. Available: www.bsn.go.id

[6] R. Agil, "Pengembangan Key Distribution Center dengan Menerapkan Protokol Kerberos dan Key Storage pada Prototipe Manajemen Kunci."

[7] S. Nepal, C. Friedrich, L. Henry, and S. Chen, "A secure storage service in the hybrid cloud," in *Proceedings - 2011 4th IEEE International Conference on Utility and Cloud Computing, UCC 2011*, 2011, pp. 334–335. doi: 10.1109/UCC.2011.55.

[8] Jv. Chandra, N. Challa, and M. Ali Hussain, "Data and Information Storage Security from Advanced Persistent Attack in Cloud Computing," 2014. [Online]. Available: http://www.ripublication.com

[9] Universitatea din Pitești, IEEE Romania Section, IEEE Industry Applications Society, and Institute of Electrical and Electronics Engineers, *Proceedings of the 10th International Conference on Electronics, Computers and Artificial Intelligence - ECAI-2018 : 28 June-30 June 2018*.

[10] D. Zhe, W. Qinghong, S. Naizheng, and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," in *2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, IEEE, May 2017, pp. 145–149. doi: 10.1109/BigDataSecurity.2017.12.

[11] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 131723–131740, 2020. doi: 10.1109/ACCESS.2020.3009876.

[12] Privacy Remix Team, "Security Analysis of Cryptsetup/LUKS," 2012. [Online]. Available: http://code.google.com/p/cryptsetup/.

[13] Indonesia, "UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 14 TAHUN 2008."

[14] BSSN, "Peraturan kepala Lembaga Sandi Negara Nomor 10 Tahun 2012 Tentang Pedoman Pengelolaan Dan Perlindungan Informasia".

[15] J. T. Harmening, "Virtual Private Networks," in *Computer and Information Security Handbook*, Elsevier, 2017, pp. 843–856. doi: 10.1016/B978-0-12-803843-7.00058-2.

[16] J. T. Harmening, "Virtual Private Networks," in *Computer and Information Security Handbook*, Elsevier Inc., 2013, pp. 855–867. doi: 10.1016/B978-0-12-394397-2.00048-9.

[17] M. Atemson Enow, "An Effective Scheme to Detect and Prevent Tampering on the Physical Layer of WSN," *Int J Sci Basic Appl Res*, [Online]. Available: http://gssrr.org/index.php?journal=JournalOfBasicAndApplied

[18] R. Vanur, "156264800." [Online]. Available: http://store.visible.com/Wiley.aspx