SISTEM *SECURITY* JARINGAN ETHERNET PADA PROTOTYPE STASIUN KERETA API YANG TERINTEGRASI DENGAN INTERLOCKING

Bahar Budi Pratama [1], Dedik Tri Istiantara [2], Bambang Gunari [3], Teguh Arifianto [4]
[1,3,4] Teknologi Elektro Perkeretaapian, Politeknik Perkeretaapian Indonesia Madiun
[2] Manajemen Teknologi Perkeretaapian, Politeknik Perkeretaapian Indonesia Madiun
bahar.tep1705@taruna.api.ac.id

ABSTRAK

Pada saat ini, pembangunan berkembang lebih cepat khususnya pada bidang transportasi salah satunya perkeretaapian. Salah satu sektor yang penting dalam pelayanan kereta api adalah sistem persinyalan kereta api. Sistem ini mengatur lalu lintas perjalanan kereta api yang berfungsi untuk memastikan kelancaran perjalanan kereta api dan menghindari terjadinya kecelakaan.

Saat ini kebanyakan meja pelayanan yang digunakan adalah meja pelayanan jenis *Local Control Panel*. Namun saat ini sudah ada meja pelayanan berbasis komputer yang umum disebut dengan meja pelayanan jenis *visual display unit* (VDU). Teknologi saat ini telah berkembang cukup pesat dan banyak ditemukan alat-alat inovasi terbaru sehingga tidak menutup kemungkinan bahwa nanti akan ada pihak yang akan menyalahgunakan hal tersebut. Untuk menangani hal tersebut dibutuhkan pengamanan sistem dari VDU tersebut baik dari data base dan keamanan jaringan yang dipakai.

Maka dilakukanlah pembuatan sistem *security* pada VDU yang dapat membantu mengamankan komunkasi VDU yang di implementasikan pada *prototype interlocking base compute.* Sistem ini dibuat menggunakan metode *whitelist,* menambahkan ip pada tiap tiap ethernet shield dengan menggunakan telnet dimana ethernet shield sebagai client dan data base sebagai server untuk keamanan tambahan ditambahkanya *(secure hash algorithm)* SHA 256 pada password untuk tambahan pengamanan komunikasi.

Dari hasil pengujian terhadap program yang sudah dibuat, dapat diambil kesimpulan bahwa sistem *security* jaringan ethernet ini dapat membantu mengamankan jaringan komunikasi. Sistem ini hanya dapat digunakan pada *prototype interlocking base computer*.

Keyword : *perjalanan kereta api, telnet, SHA256, whitelist*

1. PENDAHULUAN

Kereta api merupakan moda transportasi yang efisien untuk mengangkut jumlah penumpang yang tinggi sehingga sangat cocok untuk angkutan massal. Salah satu negara yang sedang memanfaatkan moda transportasi kereta api ini adalah Indonesia. Kereta api di Indonesia diharapkan membawa efisiensi dan efektivitas untuk transportasi maupun sistem logistik nasional. Untuk itu, inovasi dan kualitas pelayanan dalam transportasi terus ditingkatkan untuk mendorong perekonomian Indonesia.

Salah satu sektor yang penting dalam pelayanan kereta api adalah sistem persinyalan kereta api. Sistem ini mengatur lalu lintas perjalanan kereta api yang berfungsi untuk memastikan kelancaran perjalanan kereta api dan menghindari terjadinya kecelakaan. Saat ini kebanyakan meja pelayanan yang digunakan adalah meja pelayanan jenis *local control panel*. Namun saat ini sudah ada meja pelayanan berbasis komputer yang umum disebut dengan meja pelayanan jenis *Visual Display Unit* (VDU).

Selain itu, perkembangan teknologi saat ini telah berkembang cukup pesat dan banyak ditemukan alat-alat inovasi terbaru sehingga tidak menutup kemungkinan bahwa nanti akan ada pihak yang akan menyalahgunakan hal tersebut. Untuk menangani hal tersebut dibutuhkan pengamanan sistem dari VDU tersebut baik dari tampilan, data base, dan keamanan jaringan yang dipakai. Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan meskipun terkadang beberapa organisasi lebih mendahulukan tampilan dan lain sebagainya dibandingkan masalah keamanannya dan ketika sistem mendapat serangan dan terjadi kerusakan sistem, masalah dan kerugiannya akan lebih besar untuk melakukan perbaikan sistem. Maka sudah selayaknya keamanan jaringan harus lebih diperhatikan untuk melindungi sistem dari ancaman serangan yang semakin canggih dan beragam. Seperti usaha untuk membatasi akses pc *client* ke pc *server*, enkripsi untuk mengamankan data data pada setiap pc *client* maupun pc *server*.

Pada jaringan ini mengunakan topologi *star* dikarenakan menyesuaikan prinsip kerja pada prototype stasiun. Dimana server terdapat di *database* dan client terdapat di *ethernet shield*, untuk *ethernet shield* komunikasi ke *database* menggunakan *router, router* disini berfungsi sebagai *location case*. Untuk interlocking terdapat di pembuatan rute seperti jika CBI membuat rute masuk melewati JPL maka ,CBI memberi perintah ke *database* dan *database* memberi perintah ke JPL untuk menutup palang pintu, sebelum palang pintu tertutup data base tidak memberikan data tampilan pada CBI sehingga rute pada CBI yang melewati palang pintu terbentuk ketika palang pintu sudah

tertutup. Selain itu juga interlocking bekerja di rute seperti jika CBI memberi perintah ke jalur utama maka CBI akan memberi perintah ke *database*, *database* memberikan perintah ke *ethernet shield*, *ethernet shield* mengubah lampu sinyal dan penggerak wesel kemudian memberikan informasi ke *database* jika sinyal sudah terbentuk di *database* sinyal dan penggerak wesel dan ditampilkan di CBI kemudian sinyal dan penggerak wesel yang berkaitan dengan rute yang digunakan tidak akan terbentuk.

Penelitian ini membahas tentang sistem *security* jaringan ethernet pada *prototype* stasiun kereta api dimana belum ada penelitian sebelumnya. Namun penelitian yang membahas tentang *whitelist* (Pratama, dkk, 2019), dimana metode *whitelist* ini memanfaatkan sebuah port yang bisa memblok akses port kepada jaringan luar yang rentan terhadap tindakan kejahatan. Metode ini menggunakan SSH sebagai media untuk mengatur pengontrolan dari sebuah alamat IP. Alamat IP akan ditambahkan sebuah port dibelakangnya. Penggunaan block IP dengan *Operating System* Linux dan diuji melalui web dan laptop menggunakan akses *point local*.

Tujuan dari penelitan ini adalah:

a. mengetahui cara membatasi akses pada pc *server* jaringan ethernet pada *prototype* stasiun yang sudah dibuat;
b. mengetahui cara kerja telnet untuk komunikasi antara server dan client;
c. mengetahui cara membuat SHA (*Secure Hash Algorithm*) 256 sebagai keamanan tambahan pada *database*.

2. TINJAUAN PUSTAKA

Menurut Mochammad Junus (2019) metode *whitelisting* yaitu metode yang digunakan untuk menentukan IP mana saja yang diperbolehkan akses pada router yang sudah ditentukan dengan tujuan utama yaitu melindungi *database* dari serangan luar yang ilegal. Menurut Jati Sasongko (2005), metode enkripsi untuk menyandi data-data atau informasi agar tidak dapat dibaca oleh orang yang tidak berhak, sehingga yang dapat mengakses atau mengetahui hanya orang yang berhak.

Menurut Prabowo Ramadhan (2015), SHA atau *Secure Hashing Algorithm* merupakan fungsi kriptografi yang dirancang khusus oleh penyedia otoritas kemanan internet untuk menjaga keamanan data. SHA ini bekerja dengan cara melakukan transformasi data menggunakan fungsi *Hash*.

2.1 Aspek Teoritis

Telnet merupakan singkatan dari (*Telecommunications Network Protocol*), Telnet ini ialah suatu *remote login* yang terjadi pada sebuah jaringan internet yang dikarnakan oleh adanya suatu service itu dari protocol telnet. Dengan adanya sebuah telnet ini dapat/bisa memungkinkan pengguna untuk bisa mengakses komputer lain dengan menggunakan remote dengan menggunakan sebuah jaringan internet. Dan untuk pendapat yang lain mengenai telnet ialah sebuah *protocol* yang memungkinkan pengguna itu untuk dapat login serta bekerja pada sistem jarak jauh, seperti pada saat terdapat program ataupun file yang tersimpan di komputer jarak jauh yang berada pada komputer penggunanya itu sendiri. Dan pada singkatnya telnet ini merupakan perangkat lunak *(software)* yang juga digunakan untuk dapat melakukan kontrol jarak jauh pada sistem komputer.

Mac Address (Media Access Control) Address adalah sebuah alamat jaringan yang berada pada lapisan data link layer pada lapisan model OSI. Alamat ini berisi kode unik yang diberikan untuk tiap bagian dari perangkat keras jaringan komputer yang terhubung pada jaringan internet. *Mac Address* biasanya terletak pada perangkat seperti LAN *Card, Router, Wireless Card* dan perangkat lain yang menjadi bisa terhubung dengan jaringan internet.

Dalam sebuah komputer *Mac Address* ditetapkan ke sebuah kartu jaringan biasanya terletak pada *LAN Card* atau *NIC Card* dan *wireless network Card. Mac Address* sendiri memiliki panjang 48 bit yang diberikan secara unik pada perangkat keras jaringan sehingga masing-masing perangkat jaringan memiliki *Mac Address* yang tidak mungkin sama dengan perangkat yang lain. MAC terdiri atas 12 digit bilangan heksadesimal (0 s/d F), 6 digit pertama merepresentasikan vendor pembuat kartu jaringan.

Ethernet adalah teknologi jaringan komputer berdasarkan pada kerangka jaringan area lokal (LAN). Sistem komunikasi melalui *Ethernet* membagi aliran data ke dalam paket individual yang disebut frame. Setiap frame, berisi alamat sumber dan tujuan serta pengecekan error data sehingga data yang rusak dapat dideteksi dan dikirim kembali. Ethernet adalah protokol LAN yang memungkinkan setiap PC berlomba untuk mengakses network. Sekarang Ethernet menjadi protokol LAN yang paling populer karena relatif murah dan mudah di-install serta ditangani.

Enkripsi adalah bentuk modern dari kriptografi yang memungkinkan pengguna untuk menyembunyikan informasi dari orang lain. Enkripsi menggunakan algoritma yang kompleks yang disebut cipher dalam rangka untuk mengubah data normal (plaintext) menjadi serangkaian karakter acak (ciphertext) yang tidak dapat dibaca oleh orang-orang tanpa kunci khusus yang membuat data tersebut terdekripsi. Mereka yang memiliki kunci dapat mendekripsi data untuk melihat plaintext dari karakter string acak ciphertext. Dua metode enkripsi yang paling banyak digunakan adalah Public key *(asymmetric) encryption* dan *Private key (symmetric) encryption*. Keduanya sama dalam arti bahwa keduanya memungkinkan pengguna untuk mengenkripsi data untuk menyembunyikannya dari orang lain, dan

kemudian mendekripsi data tersebut dalam rangka untuk mengakses plaintext asli. Namun, mereka berbeda dalam cara mereka menangani langkah antara enkripsi dan dekripsi.

SHA atau *Secure Hashing Algorithm* merupakan fungsi kriptografi yang dirancang khusus oleh penyedia otoritas kemanan internet untuk menjaga keamanan data. SHA ini bekerja dengan cara melakukan transformasi data menggunakan fungsi Hash

Hash merupakan algoritma yang terdiri dari operasi *bitwise* (ini berkaitan dengan fungsi besaran bit enkripsi), penambahan modular dan fungsi kompresi. Fungsi hash akan menghasilkan fungsi acak yang tidak terlihat seperti aslinya.

Fungsi Hash merupakan fungsi satu arah yang tidak dapat diubah menjadi nilai hash masing-masing data tergantung tingkat bit enkripsi yang akan digunakan. Masing-masing SHA memiliki tingkat enkripsi yang berbeda dengan tingkat kerentanan yang berbeda.

Aplikasi umum SHA adalah melakukan enkripsi kata sandi dengan mengacak hash penggunaan pengiriman data tertentu dengan sandi yang sebenarnya. Jika terjadi peretasan, maka SHA akan melindungi dengan memberikan hash yang tidak dapat dibaca tanpa adanya dekripsi atau sandi asli.

Ada tiga tahapan yang dilakukan oleh algoritma hash ini dalam melakukan enkripsi data yakni ketahanan, pengubahan pra gambar 1 dan resistensi tabrakan. Hal ini memastikan integritas data atau file yang akan dikirimkan pada server penerima. Ada beberapa SHA yang sering digunakan yakni SHA 1, SHA 2 dan SHA 256.

IP address adalah alamat atau identitas numerik yang diberikan kepada sebuah perangkat komputer agar komputer tersebut teridentifikasi dan dapat berkomunikasi dengan komputer lain. Alamat atau identitas tersebut berupa nomer yang terdiri dari 4 blok bilangan desimal yang nilainya terbatas dari angka 0 sampai 255.

Whitelisting adalah fitur keamanan yang sering digunakan untuk membatasi dan mengontrol akses hanya untuk ip tertentu. *Whitelisting* IP memungkinkan untuk membuat daftar alamat IP tertentu atau rentang IP tempat pengguna dapat mengakses domain yang sudah ditentukan.

3. METODE PENELITIAN

3.1 Studi Literatur

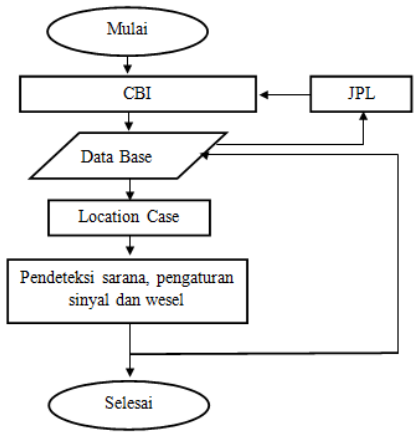
Studi Literatur yang merupakan teknik pengumpulan data atau informasi dengan mempelajari buku yang berisi konsep dan implementasi *hash* sebagai dasar dari pengembangan penulisan naskah ini.

3.2 Perancangan

Perancangan program dengan menggunakan Telnet sebagai komunikasi antara server dan client, whitelist sebagai pembatasan akses dan keamanan tambahan sistem menggunakan Hash yang khususnya yaitu SHA *(secure hash algorithm)* 256. Sistem ini akan dipasang pada *prototype* stasiun yang sudah terintegrasi dengan *interlocking*. Sistem ini berfungsi untuk melindungi dan mengamankan data-data sensitif seperti *password*. Meskipun berada di tangan orang lain data-data akan tetap aman karena mereka tidak akan tahu isinya.

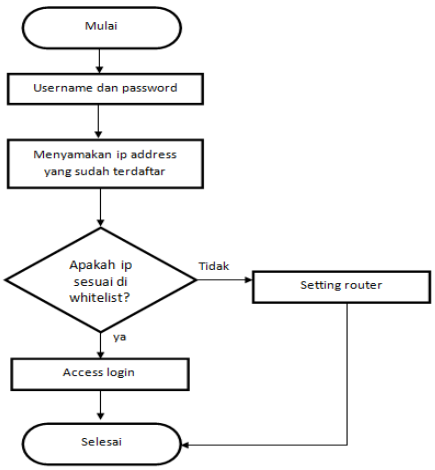
Tabel 1. IP yang dimasukan di *whitelist* pada router

No	IP Address	Type
1	24.24.24.1	Dynamic
2	24.24.24.210	Dynamic



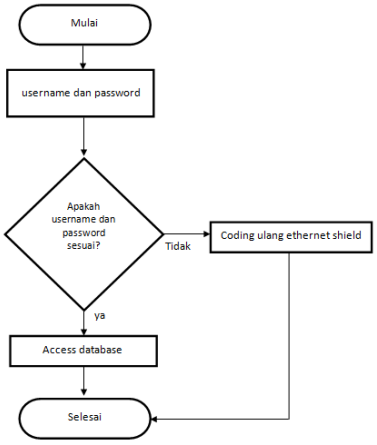
Gambar 1. *Flowchart interlocking base computer*

Dari *flowchart* diatas dapat dilihat cara kerja alat *interlocking base computer*. Dari awal yaitu saat membuka tampilan VDU selanjutnya memberikan perintah masuk ke data base setelah itu dilanjutkan ke *location case* melalui kabel Ethernet dan *router* kemudian dilanjutkan ke peralatan luar untuk menjalankan perintah. Setelah peralatan luar menjalankan perintah lalu melaporkan kondisi ke data base dan diteruskan untuk ditampilkan di VDU. Untuk JPL sendiri ketika CBI membuat rute melewati JPL, CBI memberi perintah ke data base dan data base memberi perintah ke JPL untuk menutup palang, sebelum palang pintu tertutup data base tidak memberikan data tampilan pada CBI sehingga rute pada CBI yang melewati palang pintu terbentuk ketika palang pintu sudah tertutup. Dari sistem diatas maka akan digunakan topologi sistem jaringan star sedangkan untuk komunikasinya sendiri menggunakan telnet dimana untuk clientnya terdapat pada ethernet shield dengan ID dan *password* yang sudah dienkripsi kemudian untuk servernya terdapat di databasenya sehingga jika ID dan *password* sesuai dengan yang di data base maka akan bisa saling komunikasi.



Gambar 2. *Flowchart whitelist* pada *router*

Dari *flowchart whitelist* diatas dapat dilihat cara kerja sistem *security* pada router. Saat pc ingin mengakses atau menjalankan aplikasi makan pc tersebut harus login terlebih dahulu, saat login IP dari PC akan disesuaikan dengan IP yang sudah terdaftar pada *whitelist router* yang ada, jika IP PC tersebut sudah terdaftar atau sesuai dengan *whitelist* yang ada maka PC mendapatkan akses login namun jika IP dari PC tersebut belum terdaftar makan harus menyetting router terlebih dahulu untuk mendaftarkan IP PC tersebut ke *whitelist router* agar PC tersebut bisa mendapatkan akses.



Gambar 3. *Flowchart ethernet shield*

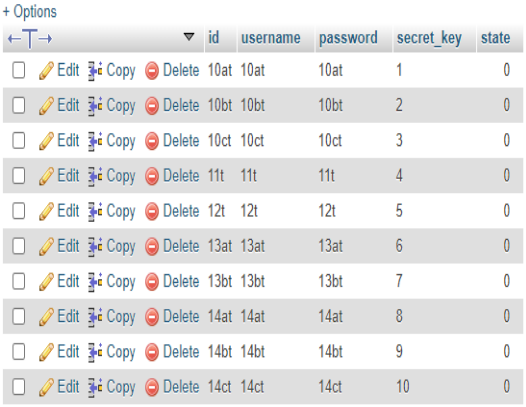
Dari *flowchart ethernet shield* di atas dapat dilihat cara kerja sistem komunikasi pada *ethernet shield*. Saat server ingin mengakses atau menjalankan komunikasi maka pc *client* tersebut harus menyesuaikan dengan IP dan *password* yang sudah terdaftar pada *server* yang ada, jika IP dan *password client* tersebut sudah sesuai dengan *server* maka client mendapatkan akses komunikasi data base namun jika IP dan *password* dari PC tersebut belum sama makan harus menkoding ulang untuk menyamakan IP dan *password* pada *server* dan *client* terlebih dahulu agar PC tersebut bisa mendapatkan akses.

3.3 Pemrograman Sistem *Security*

Pemrograman sistem *security* menggunakan bahasa pemrograman java dan dibagi menjadi beberapa bagian yaitu

1. *Password* pada *track circuit*

   Pemrograman modul ini dimulai dengan pemberian nama pada masing-masing bagian *track circuit* sesuai ID kemudian dilanjutkan dengan pemberian *password* yang berbeda dan acak.



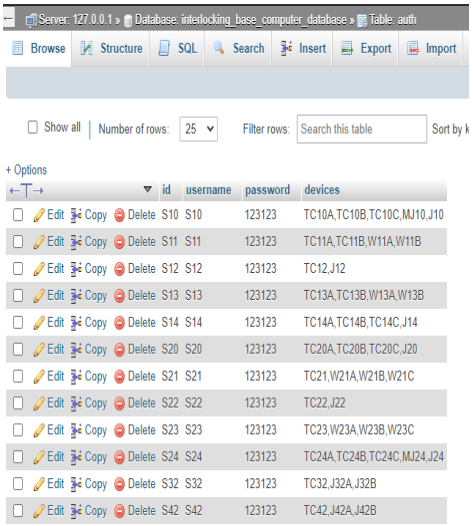
+ Options

	id	username	password	secret_key	state
Edit Copy Delete	10at	10at	10at	1	0
Edit Copy Delete	10bt	10bt	10bt	2	0
Edit Copy Delete	10ct	10ct	10ct	3	0
Edit Copy Delete	11t	11t	11t	4	0
Edit Copy Delete	12t	12t	12t	5	0
Edit Copy Delete	13at	13at	13at	6	0
Edit Copy Delete	13bt	13bt	13bt	7	0
Edit Copy Delete	14at	14at	14at	8	0
Edit Copy Delete	14bt	14bt	14bt	9	0
Edit Copy Delete	14ct	14ct	14ct	10	0

Gambar 4. Password *track circuit*

2. *Password* pada interlocking

   Pemrograman modul ini dimulai dengan pemberian nama pada masing-masing devices sesuai ID yang sudah dikelompokan dengan beberapa *track circuit*, jalur dan sinyal pada *prototype* stasiun yang sudah sesuai dengan pembuatan rute yang nantinya akan dilewati dan dibagi kemudian dilanjutkan dengan pemberian *password* yang berbeda dan acak



Server: 127.0.0.1 » Database: interlocking_base_computer_database » Table: auth

Browse Structure SQL Search Insert Export Import

Show all | Number of rows: 25 | Filter rows: Search this table | Sort by k

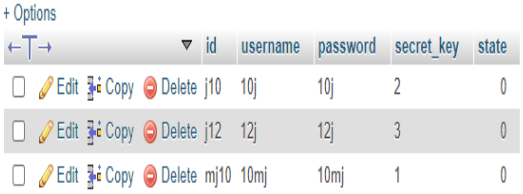
+ Options

	id	username	password	devices
Edit Copy Delete	S10	S10	123123	TC10A,TC10B,TC10C,MJ10,J10
Edit Copy Delete	S11	S11	123123	TC11A,TC11B,W11A,W11B
Edit Copy Delete	S12	S12	123123	TC12,J12
Edit Copy Delete	S13	S13	123123	TC13A,TC13B,W13A,W13B
Edit Copy Delete	S14	S14	123123	TC14A,TC14B,TC14C,J14
Edit Copy Delete	S20	S20	123123	TC20A,TC20B,TC20C,J20
Edit Copy Delete	S21	S21	123123	TC21,W21A,W21B,W21C
Edit Copy Delete	S22	S22	123123	TC22,J22
Edit Copy Delete	S23	S23	123123	TC23,W23A,W23B,W23C
Edit Copy Delete	S24	S24	123123	TC24A,TC24B,TC24C,MJ24,J24
Edit Copy Delete	S32	S32	123123	TC32,J32A,J32B
Edit Copy Delete	S42	S42	123123	TC42,J42A,J42B

Gambar 5. Password *interlocking*

3. *Password* pada sinyal

Pemrograman modul ini dimulai dengan pemberian nama pada masing-masing bagian sinyal sesuai ID kemudian dilanjutkan dengan pemberian *password* yang berbeda dan acak.



Gambar 6. Password sinyal

4. *Whitelisting* IP address

Pengaturan *whitelist* ini dimulai dengan mengubah filter mode ke *whitelist* dilanjutkan dengan memasukan IP address dari pc yang akan didaftarkan atau yang akan diberi akses di *whitelisted* MAC Address.

3.4 Pengujian Sistem Proteksi

Dalam pembuatan sistem ini harus melalui tahap pengujian, setelah sistem jadi maka harus dilakukan pengujian. sistem ini dikatakan berhasil apabila hasil pengujian sesuai dengan harapan, tetapi sistem dikatakan belum berhasil apabila hasil pengujian tidak sesuai dengan harapan. Ketika hasil pengujian belum sesuai dengan harapan, maka akan dilakukan pengecekan ulang sistem security pada jaringan ethernet ini. Setelah hasil sesuai maka akan dibuat kesimpulan dan saran dari pembuatan sistem tersebut.

Dalam penelitian ini pengujian sistem dibagi menjadi dua bagian yaitu :

a) pengujian sistem dilakukan dengan menguji apakah sistem bekerja sesuai yang diinginkan dengan mensimulasikan melalui *prototype* stasiun yang sudah dibuat;
b) pengujian sistem dilakukan dengan percobaan akses lebih dari satu kali dan mengunakan IP address yang sudah terdaftar di *whitelist* maupun tidak.

4. HASIL DAN PEMBAHASAN

4.1 Hasil Pembuatan Sistem

Sistem *security* jaringan ethernet ini dibuat untuk memberikan perlindungan terhadap data-data yang bersifat privasi terhadap pengguna asing atau yang tidak mempunyai hak. Selain itu dikarenakan menggunakan telnet maka sistem ini juga memungkinkan pengguna untuk bisa mengakses komputer lain dengan menggunakan remote dengan menggunakan sebuah jaringan internet dan untuk pendapat yang lain mengenai telnet ialah sebuah *protocol* yang memungkinkan pengguna itu untuk dapat login serta bekerja pada sistem jarak jauh, seperti pada saat terdapat program ataupun file yang tersimpan di komputer jarak jauh yang berada pada komputer penggunanya itu sendiri.

Untuk menambah pengamanan sistem digunakanlah metode *whitelist* dimana hanya ip tertentu yang bisa login, meskipun begitu ip yang sudah terdaftar tersebut hanya bisa login dengan maksimal kesalahan input password ataupun ID sebanyak 1 kali dan jika melebihi batas yang sudah ditentukan maka IP tersebut akan terblock sehingga membutuhkan konfirmasi lagi dari awal untuk memberikan izin agar ip yang terblock tersebut bisa kembali *login*.

4.2 Hasil pengujian sistem

Pada program *visual display* unit ini dilakukan pengujian agar dapat meyakinkan bahwa sistem ini dapat berjalan sesuai dengan yang diinginkan. Pengujian yang dilakukan pada sistem ini antara lain:

a. Pengujian fungsi peralatan

Tabel 2. Pengujian peralatan

Pengujian	Hasil Pengujian
Ethernet shield	*Ethernet shield* dapat bekerja dengan baik.
Router	Router dapat bekerja dengan baik.

b. Pengujian fungsi modul pada sistem *ethernet shield*

Tabel 3. Pengujian modul

Ethernet Shield	***Username***	***Password***	**Keterangan**
S10	S10	123123	IP Terhubung
S11	S11	123123	IP Terhubung
S12	S12	123123	IP Terhubung
S13	S13	123123	IP Terhubung
S14	S14	123123	IP Terhubung
S20	S20	123123	IP Terhubung
S21	S21	123123	IP Terhubung
S22	S22	123123	IP Terhubung
S23	S23	123123	IP Terhubung
S24	S24	123123	IP Terhubung
S32	S23	123123	IP Terhubung
S42	S42	123123	IP Terhubung
S10	S10	123123	IP Terhubung
S11	S11	123123	IP Terhubung
S12	S12	123123	IP Terhubung
S13	S13	123123	IP Terhubung
S14	S14	123123	IP Terhubung
S20	S20	123123	IP Terhubung
S21	S21	123123	IP Terhubung
S22	S22	123123	IP Terhubung
S23	S23	123123	IP Terhubung
S24	S24	123123	IP Terhubung
S32	S23	123123	IP Terhubung
S42	S42	123123	IP Terhubung
S10	S10	123123	IP Terhubung
S11	S11	123123	IP Terhubung
S12	S12	123123	IP Terhubung
S13	S13	123123	IP Terhubung

S14	S14	123123	IP Terhubung
S20	S20	123123	IP Terhubung
S21	S21	123123	IP Terhubung
S22	S22	123123	IP Terhubung
S23	S23	123123	IP Terhubung
S24	S24	123123	IP Terhubung
S32	S23	123123	IP Terhubung
S42	S42	123123	IP Terhubung
S10	S10	123123	IP Terhubung
S11	S11	123123	IP Terhubung
S12	S12	123123	IP Terhubung
S13	S13	123123	IP Terhubung
S14	S14	123123	IP Terhubung
S20	S20	123123	IP Terhubung
S21	S21	123123	IP Terhubung
S22	S22	123123	IP Terhubung
S23	S23	123123	IP Terhubung
S24	S24	123123	IP Terhubung
S32	S23	123123	IP Terhubung
S42	S42	123123	IP Terhubung
S10	S10	123123	IP Terhubung
S11	S11	123123	IP Terhubung
S12	S12	123123	IP Terhubung
S13	S13	123123	IP Terhubung
S14	S14	123123	IP Terhubung
S20	S20	123123	IP Terhubung
S21	S21	123123	IP Terhubung
S22	S22	123123	IP Terhubung
S23	S23	123123	IP Terhubung
S24	S24	123123	IP Terhubung
S32	S23	123123	IP Terhubung
S42	S42	123123	IP Terhubung

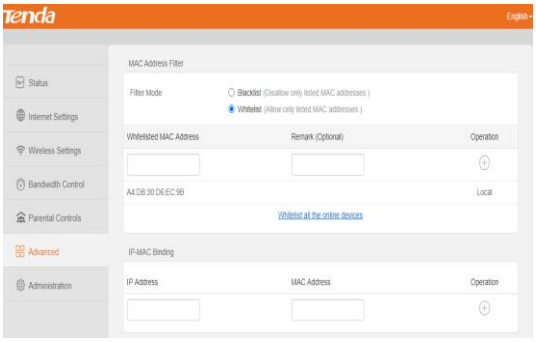
Dari table pengujian ethernet shield di atas dapat dilihat dari 5 (lima) kali pengujian pada setiap bagian modul dari ethernet shield didapatkan tidak mengalami kegagalan dalam percobaan, dikarenakan modul tidak akan salah dalam menjalankan fungsinya. Jika terdapat kesalahan besar kemungkinan salah dalam memasukan coding ke ethernet shield. Selain itu untuk komunikasi antara *server* dan *client* dapat berjalan dengan baik.

Tabel 4. Pengujian komunikasi

IP Address	bytes (m/s)				
24.24.24.1	0	0	1	0	1
24.24.24.210	0	1	0	0	1
24.24.24.211	0	0	0	0	0
24.24.24.212	0	0	0	1	1
24.24.24.213	0	1	1	1	1
24.24.24.214	0	0	1	1	1
24.24.24.220	0	0	0	0	0
24.24.24.221	0	0	0	0	0
24.24.24.222	0	0	0	0	0
24.24.24.223	0	1	1	1	1
24.24.24.224	0	1	0	1	1
24.24.24.232	0	0	1	1	1
24.24.24.242	0	0	0	0	0

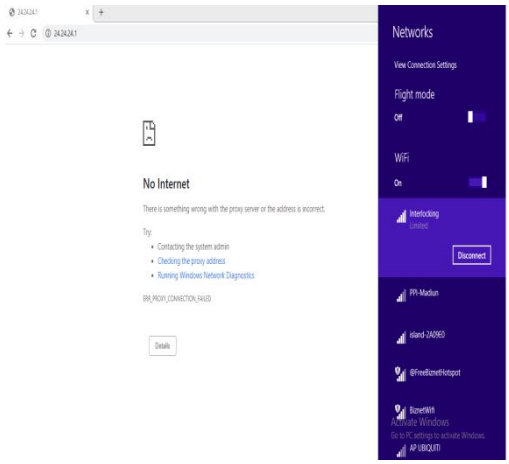
Komunikasi berjalan dengan baik dengan bytes rata rata kurang dari 1 m/s, maksimum 1 dan minimum 0.

c. Pengujian *whitelist*



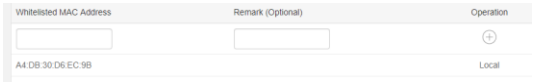
Gambar 7. IP dapat *access router*

Dari contoh pengujian IP di atas (Gambar 7) adalah contoh gambar pada IP address yang sudah terdaftar di *whitelist* sehingga bisa terhubung dengan router dan mendapatkan akses pengaturan.



Gambar 8. IP tidak dapat *access router*

Dari contoh pengujian IP di atas (Gambar 8) adalah IP address yang belum terdaftar di dalam whitelist sehingga pada gambar tersebut merupakan IP yang tidak memperoleh akses pada router.



Gambar 9. Daftar IP terhubung

Dari contoh data di atas merupakan daftar IP *address* yang sudah terdaftar setelah melalui beberapa percobaan dan pengaturan agar IP tersebut bisa saling komunikasi.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari pengujian alat terhadap sistem *security* jaringan *ethernet* dapat diambil kesimpulan yaitu:

a. pada percobaan penambahan IP *address* ke *whitelist*, penambahan IP *address* dapat dilakukan dengan baik dan PC mendapatkan akses;

b. pada percobaan penghapusan IP address yang awalnya sudah terdaftar, IP address yang telah dihapus dari *whitelist* tidak dapat diakses yang menandakan sistem dapat berjalan dengan baik;
c. untuk kemanan berlapis ini ditambahkan *username* dan *password* yang sudah terenkripsi pada ethernet shield. Pada percobaan modul dari ethernet shield sendiri dari mencoba memasukan *username* dan *password* sebanyak 5 (lima) kali, modul tersebut tidak mengalami kegagalan dan dapat terjalin komunikasi dengan baik sehingga berjalan sesuai rencana. Selain itu untuk *database* dapat membaca dan dapat menerima perintah dari VDU.

5.2 Saran

Untuk pengembangan penelitian selanjutnya yaitu:

a. penambahan enkripsi *password* untuk wesel dan sinyal sehingga *database* pada *interlocking* dapat terenkripsi dengan baik;
b. pengembangan desain agar sistem dapat berjalan secara maksimal;
c. untuk metode *whitelist* bisa dikembangkan menjadi metode lain yang lebih aman dan modern.

DAFTAR PUSTAKA

[1] Prabowo, R. T., Kurniawan, M. T. 2015. 'Analisis dan Desain Keamana Jaringan Komputer dengan Metode *Network Development Life Cycle* (Studi Kasus: Universitas Telkom)'. *Jurnal Rekayasa Sistem & Industri*. Vol.2, No.1, hh.1-7.

[2] Pratama, J. A., Heru, Y., dan Junus, M. 2019. 'Implementasi Keamanan Jaringan dengan Metode *Whitelist* pada Server Jurusan Elektro di Politeknik Negeri Malang'. *Jurnal Jaringan Telekomunikasi*. Vol.8, No.1, hh.66-71.

[3] Sasongko, J. 2005. 'Pengamanan Data Informasi Menggunakan Kriptografi Klasik'. *Jurnal Dinamik*. Vol.10, No.3, hh.160-167.

[4] Sirait, E. R. E. 2016. 'Respon Masyarakat Terhadap Sistem *Whitelist*: Al;ternatif untuk Akses Internet yang Lebih Aman'. *Jurnal Penelitian dan Pembangunan*. Vol.17, No.2, hh.127-142.

[5] Hendratno, E. 2017. *8 Software Simulator jaringan keren dan menarik untuk belajar jaringan*. Diakses tanggal 07 September 2020.

[6] Stallings, W dan Brown, L. 2018. *Computer Security: Principles and Practice, 4th Edition*. Pearson.