J-Com (Journal of Computer) ISSN 2775-801X (Online)
Vol. 1 No. 2, Juli 2021, hlm. 95 – 102
DOI: https://doi.org/10.33330/j-com.v2i1.1206
Available online at http:// jurnal.stmikroyal.ac.id/index.php/j-com

PERANCANGAN SISTEM KEAMANAN *FILE TRANSFER PROTOCOL* DENGAN *SECURE SOCKET LAYER* PADA *SERVER CENTOS* 7

Alexander Theo Philus Tambunan [1], Adi Prijuna Lubis [2*], Syartika Anggraini [3]
[1]Mahasiswa Prodi Sistem Komputer, STMIK Royal
Prodi Sistem Komputer, STMIK Royal
**email*: pri7n4@gmail.com

Abstract: An advancement in communication technology currently has an influence on developments in data management in the joints of life, making the need for a media center something a must in digital archive storage. Data will not always be stored in personal computers, but it would be better if there was a centralized data container to be a solution in storage media, in order to prevent data loss or data backup. The term network (network) is used when there are at least two or more devices that are connected to one another. To carry out data exchange in this network, a protocol is used that specifies how data is exchanged, and one of the most widely used protocols is the File Transfer Protocol (FTP). FTP is generally useful as a means of exchanging files or data in a network. The FTP protocol is not secure enough, because when data transfer there is no security to protect it. Therefore the FTP protocol is necessary for additional security, by implementing the SSL security protocol or Secure Socket Layer Security protecting the FTP protocol during data transfer. SSL certificates are used for the purpose of handling the security of data packets transmitted over the network system. When SSL is activated, the server and client when the connection occurs will be encrypted so that the data cannot be seen by others.

Keywords: FTP; Network; Server; SSL

Abstrak: Suatu Kemajuan teknologi komunikasi saat ini memiliki pengaruh terhadap perkembangan didalam pengelolaan data didalam sendi kehidupan, membuat kebutuhan akan media center menjadi sesuatu yang harus dalam penyimpanan arsip digital. Data tidak selamanya akan tersimpan di dalam personal computer saja tetapi akan lebih baik jika ada wadah data terpusat menjadi solusi dalam media penyimpanan, agar menjaga dari kehilangan data atau cadangan data. Istilah jaringan (network) dipakai apabila terdapat minimal dua atau lebih perangkat yang terhubungkan satu dengan yang lainnya. Untuk melaksanakn pertukaran data didalam jaringan ini, digunakan protocol yang menspesifikasikan bagaimana data dipertukarkan, dan salah satu protocol yang banyak digunakan adalah File Transfer Protocol (FTP). FTP umumnya bermanfaat sebagai sarana pertukaran file atau data dalam suatu network. Protokol FTP tidaklah cukup aman, dikarenakan ketika transfer data tidak ada keamanan untuk melindunginya. Maka dari itu protokol FTP perlu untuk penambahan keamanan, dengan menerapkan protokol keamanan SSL atau Secure Socket Layer Security melindungi protokol FTP pada saat transfer data. Sertifikat SSL dimanfaatkan untuk keperluan menangani keamanan paket data yang ditransmisikan melalui sistem jaringan. Ketika SSL diakatifkan, maka server dan client ketika terjadi koneksi akan ter enkripsi sehingga data yang ada tidak dapat untuk dilihat oleh orang lain.

Kata kunci: FTP;Network; Server;SSL

J-Com (Journal of Computer) ISSN 2775-801X (Online)
Vol. 1 No. 2, Juli 2021, hlm. 95 – 102
DOI: https://doi.org/10.33330/j-com.v2i1.1206
Available online at http:// jurnal.stmikroyal.ac.id/index.php/j-com

PENDAHULUAN

Suatu Kemajuan teknologi komunikasi saat ini memiliki pengaruh terhadap perkembangan didalam pengelolaan data. Dimana data dari satu lokasi bisa ditransfer ke lokasi lainnya menggunakan bantuan sarana telekomunikasi. Pengiriman data lewat komputer dilaksanakan melalui media transmisi elektronik, yang sering diartikan dengan pengistilahan komunikasi data (*data communication*). Istilah jaringan *(network)* dipakai apabila terdapat minimal dua atau lebih perangkat yang terhubungkan satu dengan yang lainnya. Untuk melaksanakn pertukaran data didalam jaringan ini, digunakan *protocol* yang menspesifikasikan bagaimana data dipertukarkan, dan salah satu *protocol* yang banyak digunakan adalah *File Transfer Protocol* (FTP).

FTP dasarnya berguna sebagai *protocol* guna sarana tukar menukar *files* atau data didalam suatu *networks* yang berbasiskan koneksi TCP. FTP merupakan *protocol* pilihan yang paling cocok digunakan dalam *save files* secara cepat dan efisien dalam proses *uploads* dan *downloads* dari komputer *server* ke *client* maupun sebaliknya [1]. FTP akan dapat diakses kapan saja selama user dapat terhubung dengan jaringan lokal maupun jaringan *internet*. Saat ini FTP menjadi rentan terhadap serangan *cyber* seperti *Sniffing attack, Scanning, Man In The Midle Attac*k, DDoS dan lainnya [2]. Serangan-serangan tersebut biasanya dilakukan untuk mengetahui *username, password*, maupun file yang di-*upload* atau yang di-*download* oleh *user*. Maka dari itu dibutuhkan layanan keamanan guna menjaga komunikasi antara user dengan server. FTP *server* dapat dibekali oleh *Secure Socket Layer* (SSL) [1]. SSL dirancang untuk memberikan jaminan keamanan dan layanan kompresi ke data yang dihasilkan dari lapisan aplikasi, ini biasanya ditemukan di HTTP, sebagai keamanan data antara *transport* dan *aplication layer* [3].

Teknologi *Secure Socket Layer* menggunakan konsep kriptografi kunci publik untuk bisa mencapai komunikasi yang benar-benar aman antara *server* dan *client* [4]. Kedua pihak yang berkomunikasi (*server* dan *client*) harus saling mengirimkan data yang disamarkan dengan teknik *enkripsi*, dan untuk membaca data tersebut digunakan kunci yang hanya dimiliki oleh kedua pihak yang sedang berkomunikasi saja. Sehingga apabila ada pihak lain yang mencoba untuk menyadap, data tidak akan terbaca atau tersamarkan dalam karakter yang acak.

Pada Dinas Pendidikan Kabupaten Asahan telah dilengkapi dengan sistem jaringan yang memadai. Proses pertukaran data telah dilakukan dengan menggunakan *sharing files* antar komputer satu ke komputer lain dan juga terkadang masih menggunakan cara manual menggunakan *flashdisk*. Namun permasalahan saat ini pada Dinas Pendidikan Kabupaten Asahan belum tersedia sebuah *server* sebagai tempat penyimpanan utama dilengkapi dengan sistem keamanan yang baik. Dengan tidak dilengkapinya keamanan, pada *server* penyimpanan bagi *user, transfer* data yang *reliable* dan *efisien* maka, memungkin komputer dapat menyebarkan virus, rawan terjadinya *sniffing, modification* dan *fabrication* data.

Beberapa penelitian terdahulu telah banyak dilakukan berkaitan FTP maupun penelitian yang mengkaji penggunaan *Secure Socket Layer* (SSL) sebagai *system* keamanan didalam komunikasi jaringan, untuk menganalisa *protocol Secure Socket Layer* terhadap dua bentuk serangan yaitu *Heartbleed Bug* dan *Distributed Denial of Service* (DDoS), [5], [6]. perancangan dan implementasi data *center* menggunakan FTP,

J-Com (Journal of Computer) ISSN 2775-801X (Online)
Vol. 1 No. 2, Juli 2021, hlm. 95 – 102
DOI: https://doi.org/10.33330/j-com.v2i1.1206
Available online at http:// jurnal.stmikroyal.ac.id/index.php/j-com

diman data *center* yang dibangun pada penelitian tersebut adalah data *center* pada *server* mikrotik. [4]. merancang FTP dengan pengamanan open ssl pada jaringan VPN Mikrotik. [7] melakukan penelitian implementasi *firewall* dan *port knocking* untuk keamanan data pada FTP *server* yang berbasis *linux ubuntu server.*

Penggunaan metode FTP ini diharapkan dapat membantu mempermudah didalam penyimpanan *files* dan untuk berbagi data didalam jaringan. Selain itu penggunaan metode pengamanan dengan *Secure Socket Layer* bertujuan sebagai keamanan agar layanan yang ada menjadi aman dari penyadapan atau *sniffing packet.*

METODE

Dalam tahap perencanaan dilakukan pengumpulan data dan mempelajari landasan-landasan yang akan dibangun. Pengumpulan dilakukan berdasarkan pada studi pustaka yaitu mempelajari teori yang berkaitan dengan FTP *server* dan *Secure Socket Layer* (SSL).

Pada tahap analisis dilakukan pengidentifikasian terhadap kebutuhan penelitian. Hal ini diperlukan untuk menjadi acuan sistem yang dibangun. Kegiatan yang dilakukan dalam menganalisis yaitu memahami alur penyampaian informasi yang sedang berjalan, mengidentifikasi masalah yang terjadi pada sistem yang berjalan, dan mencari kesimpulan dari proses analisis yang telah dilakukan.

Sebuah kegiatan merancang *server* FTP dengan melakukan instalasi dan konfigurasi kemudian *server* FTP selesai di konfigurasi maka selanjutnya akan dilakukan perancangan terhadap sistem keamanan pada *server* tersebut. Aplikasi yang digunakan untuk melihat proses yang terjadi pada komunikasi yang berjalan adalah *wireshark*. Aplikasi ini dapat melihat *packet header* yang *tercapture* ketika komunikasi antara *client* dan *server* sedang berlangsung.

Uji coba sistem yaitu proses yang dilakukan untuk menilai apakah sistem yang dibuat telah sesuai dengan apa yang diharapkan, merupakan suatu kegiatan guna mengevaluasi keunggulan dan kelemahan terhadap sistem. Setelah sistem dibangun berdasarkan apa yang dirancang oleh penulis, maka penulis melakukan uji coba untuk mengevaluasi keunggulan dan kelemahan dari sistem yang telah dibangun. Ujicoba akan dilakukan dalam dua tahap dimana tahap pertama pengujian akan dilakukan pada FTP *Server* pada kondisi belum memiliki sistem keamanan, disini akan diuji dengan cara FTP *server* akan dicoba untuk di *capture packet* pada saat komunikasi antara *server* dan *client*. Kemudian pengujian kedua adalah saat FTP *server* telah dipasang *Secure Socket Layer* (SSL) pada pengujian kedua ini akan terlihat dampak dari penerapan sistem keamanan pada FTP *server* dibanding dengan kondisi sebelumnya.

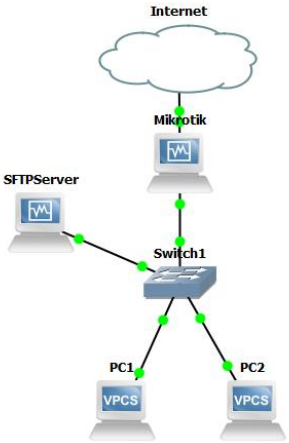
Pada tahap ini merupakan proses akhir yaitu menganalisa dan evaluasi hasil pengujian sebelumnya dalam proses ini dilakukan evaluasi dan kesimpulan terhadap kualitas sistem yang telah dibangun.

HASIL DAN PEMBAHASAN

Dengan melihat permasalahan yang terjadi di Sistem Jaringan dinas pendidikan

J-Com (Journal of Computer) ISSN 2775-801X (Online)
Vol. 1 No. 2, Juli 2021, hlm. 95 – 102
DOI: https://doi.org/10.33330/j-com.v2i1.1206
Available online at http:// jurnal.stmikroyal.ac.id/index.php/j-com

kabupaten asahan maka peneliti mengusulkan untuk membangun *Server* FTP yang akan mengatasi pertukaran data menggunakan perangkat eksternal, menyediakan keamanan data dan menyediakan tempat penyimpanan data yang *reliable* dan efisien serta memiliki sistem keamanan yang baik. Dari sistem jaringan yang berjalan pada dinas pendidikan peneliti tetap menggunakan alokasi IP Address yang sedang berjalan hanya menambahkan *IPAddress static* pada *router* untuk dipergunakan oleh *Server* FTP Adapun topologi dari sistem yang di usulkan tertera pada Gambar 1 berikut ini.



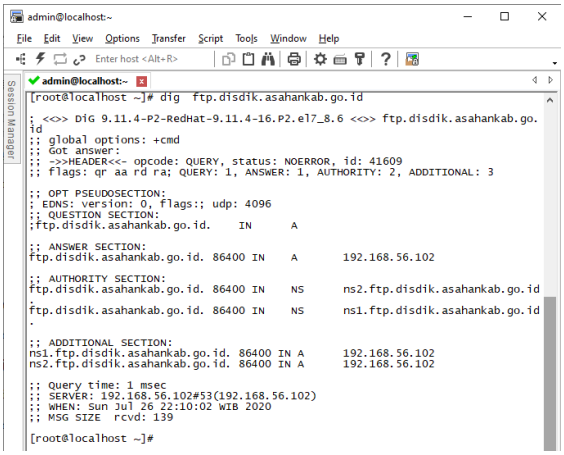
Gambar 1. Topologi Usulan

Implementasi sistem keamanan FTP dengan *Secure Socket Layer* akan diaplikasikan pada CentOS 7 *server.* Dalam pengujian ini sistem ini diimplementasikan dalam bentuk virtualisasi menggunakan *Virtual Box* yang dapat dijalankan diberbagai platform sistem operasi seperti *Windows, Linux* maupun Mac OS. Pengujian ini dilakukan menggunakan laptop untuk menjalankan *virtualisasi CentOS Server* yang telah dikonfigurasi sebagai *Domain Server,* FTP dan juga dilengkapi *protocol Secure Socket Layer.*

Pada sistem yang dibangun akan dilakukan beberapa pengujian, ini dilakukan agar sistem yang dibuat dapat berjalan sesuai dengan kebutuhan dan tujuan dalam jurnal ini. Rangkaian pengujian yang dilakukan adalah pengujian *domain server,* pengujian FTP *Server* dan pengujian keamanan FTP *Server.*

Domain Name Server atau biasa juga disingkat penyebutannya dengan DNS merupakan suatu layanan pada *server* yang berfungsi untuk mempermudah seorang *user* atau pengguna didalam mengakses suatu layanan seperti FTP *Server* maupun *Web server.* Fungsi utama dari DNS *server* sebagai penerjemah *IPAddress* kedalam bentuk kata yang unik maupun dari kata unik kedalam bentuk *IPAddress*. Dalam sistem yang telah dibuat alamat *domain name* yang dibuat adalah *ftp.disdik.asahankab.go.id.* Alamat domain ini nantinya dapat diakses secara *local* oleh *user* untuk menggunakan layanan FTP *Server* yang tersedia. Untuk pengujian *domain name* ini dapat dilakukan dengan beberapa cara, salah satunya dengan perintah ping *ftp.disdik.asahankab.go.id* melalui *command prompt* pada *windows* atau terminal pada *linux.* Selain dengan cara tersebut dapat juga dilakukan dengan cara lainnya yaitu dengan menggunakan perintah *dig ftp.disdik.asahankab.go.id* seperti yang terlihat pada gambar 2 berikut ini.

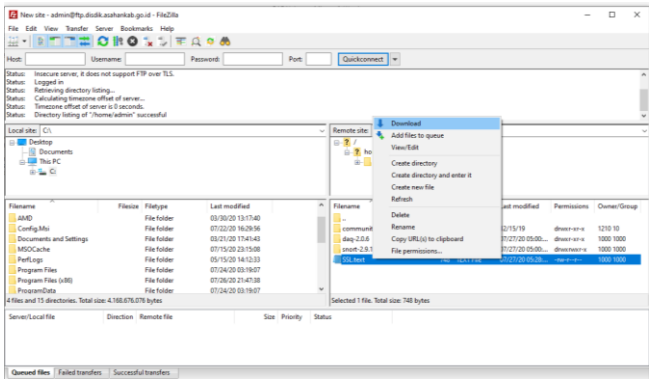
J-Com (Journal of Computer) ISSN 2775-801X (Online)
Vol. 1 No. 2, Juli 2021, hlm. 95 – 102
DOI: https://doi.org/10.33330/j-com.v2i1.1206
Available online at http:// jurnal.stmikroyal.ac.id/index.php/j-com



Gambar 2. Uji Coba *Domain Server*

Pada gambar 2 merupakan uji coba terhadap *Domain Name Server* dengan menggunakan perintah *dig ftp.disdik.asahankab.go.id*. Perintah *dig* merupakan perintah *command line* pada linux yang sangat baik. Dengan menggunakan perintah dig maka dimungkinkan untuk mengecek *record Domain Name Server* (DNS) seperti *IPAddress Domain*, *A record* dan lain sebagainya. Berdasarkan pengujian yang dilakukan pada tahap ini telah menunjukkan bahwa konfigurasi untuk *Domain Name Server* telah berhasil dan dapat digunakan.

Pengujian akses FTP *server* dilakukan dengan menggunakan aplikasi khusus yaitu *file zilla*, dengan aplikasi ini *user* dapat dengan mudah untuk mengambil atau *mendownload file* yang ada pada *server*, sesuai dengan kebutuhan yang diinginkan. Disini *user* yang mengakses FTP *server* akan diminta untuk memasukkan *password* terlebih dahulu, guna keamanan akses pada FTP *server*. Setelah user berhasil login maka user dapat menggunakan FTP *server* untuk beberapa keperluan pengambilan data dari *server* maupun menyimpan data ke *server*. Pada gambar 3 disini akan dilakukan uji coba untuk mengambil data dari *server* dengan cara men*download* data yang terdapat pada salah satu *directory* penyimpanan pada *server*.

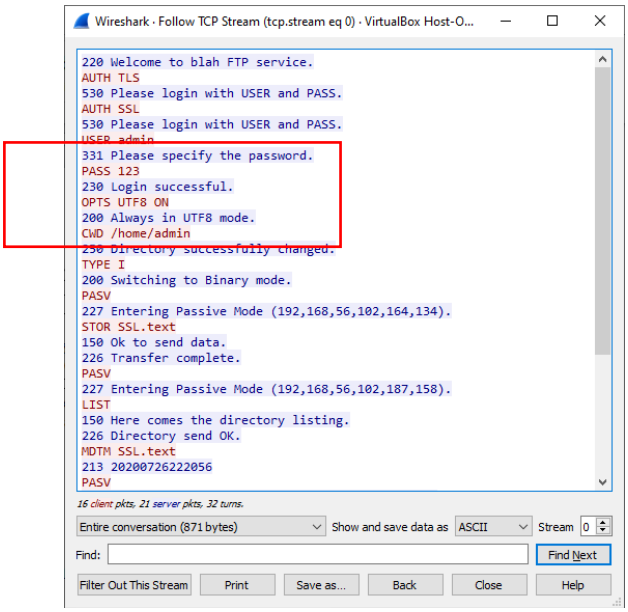


Gambar 3. Proses *Download File* Pada FTP *Server*

Selain untuk men-*download file* atau dokumen pada *server* layanan FTP juga menyediakan fasilitas *upload*, sehingga *user* juga dapat menyimpan data atau dokumennya pada FTP *server*. Untuk layanan FTP *server* telah berjalan dengan baik

J-Com (Journal of Computer) ISSN 2775-801X (Online)
Vol. 1 No. 2, Juli 2021, hlm. 95 – 102
DOI: https://doi.org/10.33330/j-com.v2i1.1206
Available online at http:// jurnal.stmikroyal.ac.id/index.php/j-com

maka selanjutnya perlu dilakukan uji coba terhadap kemanan dari layanan FTP *server* ini. Untuk menguji keamanan suatu *server* disini penulis mekukakan pembacan paket yang lewat didalam jaringan atau teknik ini juga biasa disebut dengan *sniffing*. Dengan teknik ini akan didapatkan sekumpulan proses komunikasi yang terjadi yaitu proses komunikasi didalam jaringan. Selanjutnya dari hasil tangkapan data tersebut dapat dilihat apakah komunikasi yang terjadi aman atau tidak. Misalnya ketika *user* login ke *server* FTP *user* dan *password*nya serta aktivitas yang dikerjakan dapat atau tidak dibaca oleh pihak ketiga.



Gambar 4. Hasil Pengujian Awal Keamanan FTP *Server*

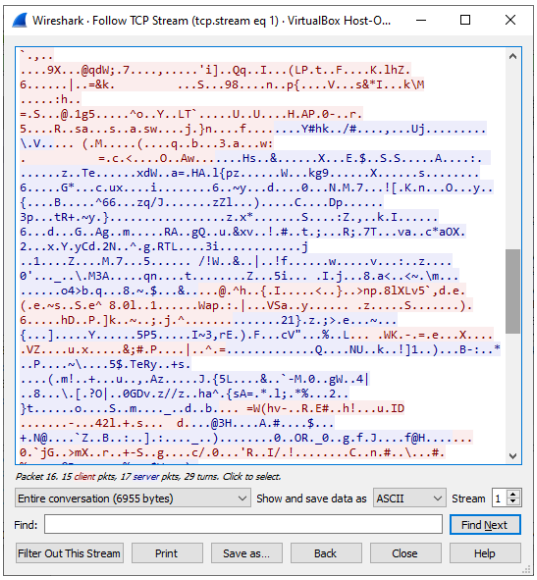
Pada gambar 4 dapat dilihat hasil *capturing packet* dengan *wireshark* pada FTP *server*, dimana dapaat dilihat sebuah fakta bahwa FTP *server* yang tidak dilengkapi dengan keamanan SSL dapat dilihat *packet* data yang di trasmisikan. Pada hasil *capturing packet* tersebut diperoleh hasil yaitu mendapatkan *user* dan *passsword* untuk admin FTP *server*. Ini terjadi dikarenakan komunikasi antara *server* dengan *client* tidak di *enkripsi* sehingga dengan dilakukan penyerangan dengan teknik *sniffing* paket data yang dikomunikasikan tersebut dapat dilihat. Pada tahapan ini *server* FTP sudah siap digunakan namun dalam komunikasinya belum aman sepenuhnya.

Pada layanan FTP *server* yang dibangun ini menggunakan sistem keamanan dengan menggunakan kriptografi algoritma RSA 2048 dalam bentuk *certifikat Secure Socket Layer* (SSL) yang dipasang pada *server*. Untuk pertama kali akses ke *server* FTP maka akan muncul satu *form* notifikasi yang menunjukkan terdapat *certifikate* yang tidak dikenal. disini setiap user yang menggunakan *filezilla* harus mendaftarkan *certificate* tersebut ke aplikasi yang digunakan agar layanan FTP *server*nya dapat digunakan dengan baik. setelah *verifikasi certificate* tersebut selesai barulah *user* dapat menggunakan layanan FTP *Server*.

Selanjutnya disini perlu diuji Kembali untuk tingkat keamanan dari FTP *Server*. Sebelumnya telah dilakukan penyadapan atau serangan *packet sniffing* ke FTP *Server* dari awal yaitu saat pertama login user login ke FTP *server*. Pada gambar 5

J-Com (Journal of Computer) ISSN 2775-801X (Online)
Vol. 1 No. 2, Juli 2021, hlm. 95 – 102
DOI: https://doi.org/10.33330/j-com.v2i1.1206
Available online at http:// jurnal.stmikroyal.ac.id/index.php/j-com

disini memperlihatkan hasil dari serangan *packet sniffing* dimana setiap data yang dikomunikasikan di FTP *Server* sudah di enkripsi sehingga data tidak lagi dapat disadap, di modification dan fabrication [9].



Gambar 5. Hasil Pengujian Keamanan FTP *Server*

SIMPULAN

Dari serangkaian penelitian dan hasil uji coba maka disini dapat disimpulkan bahwa Metode pengamanan dengan *Secure Socket Layer* (SSL) dapat di implementasikan dan berjalan dengan baik pada FTP *Server*. Keamanan *File Transfer Protocol* (FTP) dengan menggunakan *Secure Socket Layer* (SSL) secara standar terbukti dapat melindungi transmisi FTP *Server* dari Tindakan penyadapan paket data.

DAFTAR PUSTAKA

[1] D. Ruwaida and D. Kurnia, "Rancang Bangun File Transfer Protocol (Ftp) Dengan Pengamanan Open Ssl Pada Jaringan Vpn Mikrotik Di Smk Dwiwarna," *Comput. Eng. Sci. Syst. J.*, vol. 3, no. 1, p. 45, 2018, doi: 10.24114/cess.v3i1.8267.

[2] Khairunnisa and Sutarti, "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (Distributed Denial of Service) Berbasis Honeypot," *J. PROSISKO*, vol. 4, no. 2, p. 8, 2017.

[3] J. A. Habibi, R. Munadi, and L. V. Yovita, "Analysis secure socket layer protocol with heartbleed bug and distributed denial-of-service," *ICCEREC 2016 - Int. Conf. Control. Electron. Renew. Energy, Commun. 2016, Conf. Proc.*, pp. 54–59, 2017, doi: 10.1109/ICCEREC.2016.7814960.

[4] N. Novi and Z. Zaini, "Secure Socket Layer untuk Keamanan Data Rekam Medis Tumor Otak pada Health Information System," *J. Nas. Tek. Elektro*, vol. 6, no. 3,

p. 137, 2017, doi: 10.25077/jnte.v6n3.405.2017.

[5] D. Q. Shengrong Mao, "Design and Implementation of An Embedded FTP Server Powered over Ethernet Shengrong Mao, Donghai Qiao," pp. 2421–2424, 2016.

[6] B. Kurniawan and D. Herryanto, "Perancangan Dan Implementasi Data Center Menggunakan File Transfer Protocol (Ftp)," *Peranc. Dan Implementasi Data Cent. Menggunakan File Transf. Protoc.*, vol. 2, no. 2, pp. 91–97, 2017, doi: 10.1360/zd-2013-43-6-1064.

[7] S. Khadafi, S. Nurmuslimah, and F. K. Anggakusuma, "Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server," vol. 4, no. 3, pp. 181–188, 2019.

[8] A. R. Adiguna, M. Saputra Chandra, and F. Pradana, "Analisis dan Perancangan Sistem Informasi Manajemen Gudang pada PT Mitra Pinasthika Mulia Surabaya," *Pengantar Sist. Inf.*, vol. 2, no. 2, pp. 612–621, 2018, doi: 10.1016/j.humimm.2008.04.008.

[9] S. Prabhakar, "Research in Computer Applications and Robotics Network Security in Digitalization : Attacks and," vol. 5, no. 5, pp. 46–52, 2017.