ROUTERS: Jurnal Sistem dan Teknologi Informasi
Vol. 2, No. 2, Juli 2024, pp. 70-78
ISSN: 2962-1224, DOI: 10.25181/rt.v2i2.3328

Autentikasi *User* Dengan Metode *Single Sign-On* Berbasis *Windows Active Directory* Pada PT. XYZ

Kemas Ocha Khairi Saputra[1], Agiska Ria Supriyatna[2], Septafiansyah Dwi Putra[3]
[1] Program Studi Manajemen Informatika, Politeknik Negeri Lampung
[2,3] Program Studi Teknologi Rekayasa Internet, Politeknik Negeri Lampung

INFORMASI ARTIKEL

Diterima 1 November 2023
Direvisi 5 November 2023
Diterbitkan 17 Januari 2024

Kata kunci:

Autentikasi;
Single Sign-On;
Active Directory;

ABSTRAK

Untuk terhubung ke dalam jaringan perusahaan terdapat sistem keamanan berbasis WPA2-PSK sehingga *user* diwajibkan memasukan *password* wifi perusahaan. Salah satu isu yang muncul adalah kesulitan dalam mengidentifikasi status *user* yang berupaya mengakses jaringan. Selain permasalahan dari segi keamanan jaringan, dengan pengunaan *key security* tersebut *user* selain karyawan dapat terhubung ke jaringan menggunakan perangkat pribadi. Sebagai salah satu solusi untuk memperbaiki sistem autentikasi yang ada pada saat ini, terdapat sistem keamanan yang dapat dimanfaatkan seperti RADIUS. Sistem dijalankan untuk menghindari ancaman pada sistem keamanan jaringan. Proses yang dilakukan dengan menerapkan metode NDLC ini dimulai dengan mengidentifikasi dan melakukan perancangan autentikasi keamanan pada jaringan sampai ke tahap implementasi rancangan tersebut hingga dapat digunakan secara rutin. Dengan adanya sistem autentikasi *user* dengan metode *single sign-on* berbasis *Windows active directory* pada PT. XYZ *user* akan lebih mudah untuk terhubung ke dalam jaringan *wireless*. Dengan WPA2 - *Enterprise* akses untuk masuk ke dalam jaringan akan terbatas.

User Authentication Through Windows Active Directory-Based Single Sign-On Method at PT. XYZ

ARTICLE INFO

Received November 1, 2023
Revised November 5, 2023
Published January 17, 2023

Keyword:

Authentication;
Single Sign-On;
Active Directory;

ABSTRACT

To connect to the company network, a WPA2-PSK-based security system is in place, requiring users to input the company's Wi-Fi password. One of the issues that arises is the difficulty in identifying the status of users attempting to access the network. Apart from security concerns regarding the network, the use of this security key allows non-employees to connect to the network using personal devices As a solution to enhance the existing authentication system, security systems like RADIUS can be utilized. This system operates to mitigate threats to network security. The process undertaken through the implementation of this NDLC method commences with identifying and designing network security authentication, progressing through the implementation phase until the design can be regularly utilized. With the introduction of a user authentication system employing a single sign-on method based on Windows Active Directory at XYZ Inc., users will find it easier to connect to the wireless network. With WPA2-Enterprise, access to the network will be restricted

Corresponding Author:

Kemas Ocha Khairi Saputra, Politeknik Negeri Lampung
Email: ochakhairi65@gmail.com

1. PENDAHULUAN

PT. XYZ merupakan salah satu perusahaan yang bergerak dibidang energi. Pada proses kegiatan operasional perusahaan, masing – masing divisi memerlukan koneksi jaringan wireless untuk terhubung ke internet. Untuk terhubung ke dalam jaringan perusahaan terdapat sistem keamanan berbasis WPA2-PSK sehingga *user* diwajibkan memasukan *password* wifi perusahaan. WPA2-PSK merupakan metode keamanan jaringan *wireless*, WPA2-PSK menggunakan dua tipe enkripsi yaitu *Advanced Encryption Standard* (AES) dan *Temporal Key Integrity Protocol* (TKIP)[1]. Salah satu isu yang muncul adalah kesulitan dalam mengidentifikasi status *user* yang berupaya mengakses jaringan. Selain permasalahan dari segi keamanan jaringan, dengan pengunaan *key security* tersebut *user* selain karyawan dapat terhubung ke jaringan menggunakan perangkat pribadi. Dampak dari kegiatan tersebut akan membuat IP *lease* yang ada pada DHCP *Server* menjadi penuh.

Sebagai salah satu solusi untuk memperbaiki sistem autentikasi yang ada pada saat ini, terdapat sistem keamanan yang dapat dimanfaatkan seperti RADIUS. Sistem RADIUS akan digunakan sebagai salah satu metode keamanan yang akan diterapkan pada tugas akhir ini. RADIUS merupakan sebuah standar keamanan komputer yang penerapannya ditujukan untuk melakukan otentikasi, otorisasi, dan pendaftaran akun *user* secara terpusat [2]. Beberapa masalah keamanan yang diteumui terkait autentikasi telah dikaji pada penelitian sebelumnya seperti pada *smartcard*[3], layanan[4], sistem enkripsi[5], [6], [7] dan IoT [8], [9].

Tujuan tugas akhir ini adalah menghasilkan sistem autentikasi *user* dengan metode *single sign-on*. Sistem dijalankan untuk menghindari ancaman pada sistem keamanan jaringan. Kendala seperti lupa *password* ketika ingin terhubung ke dalam jaringan atau IP *addres* pada DHCP *server* yang penuh akan teratasi dengan adanya sistem autentikasi metode *single-sign on.*

2. METODE

Metode pelaksanaan yang penulis terapkan untuk pembuatan tugas akhir ini adalah dengan meng implementasikan metode NDLC yang merupakan singkatan dari *Network Development Life Cyle. Network Development Life Cyle atau biasa disingkat dengan sebutan NDLC adalah sebuah metode yang bermanfaat untuk pengembangan jaringan yang ada dengan menjalankan beberapa proses seperti analisis, desain, simulasi, implementasi, monitoring, sampai manajemen* [10]. Proses yang dilakukan dengan menerapkan metode NDLC ini dimulai dengan mengidentifikasi dan melakukan perancangan autentikasi keamanan pada jaringan sampai ke tahap implementasi rancangan tersebut hingga dapat digunakan secara rutin.

2.1. Analisis

Pada tahapan ini langkah awal yang diperlukan adalah mengumpulkan informasi yang akan berguna sebagai data dalam tindakan apa saja yang akan dilakukan. Di tahapan ini penulis akan mengobservasi keluhan *user* yang ada pada PT. XYZ dan kendala yang dialami oleh tim IT ketika melakukan monitoring jaringan. Informasi yang didapatkan dari narasumber akan dianalisis dan menjadi data untuk langkah berikutnya.

2.2. Desain

Pembuatan desain akan dilakukan dengan menampilkan gambar dari sistem *login wireless* yang di rancang. Desain dibuat sesuai dengan kebutuhan sistem autentikasi *user* dengan *single sign-on* yang akan di terapkan pada PT. XYZ.

2.3. Simulasi

Simulasi yang akan dibuat pada tahapan ini akan menggunakan *cisco packet tracer*. Pada simulasi terdapat gambaran sistem yang berjalan dari toplogi yang dibuat. Alur sistem yang berjalan mulai dari tahapan *user* ke sistem autentikasi akan di tampilkan pada simulasi agar proses berjalannya terdefinisikan dengan jelas.

2.4. Implementasi

Pada tahapan implementasi ini sistem autentikasi *user* dengan metode *single sign-on* berbasis *Windows active directory* pada PT. XYZ akan diterapakan pada lingkungan jaringan yang ada. Aspek penting yang perlu diperhatikan ketika melakukan kegiatan ini adalah memastikan kompatibilitas pada perangkat jaringan yang ada dapat menerima sistem autentikasi dengan metode *single sign-on* dengan baik dan lancar.

2.5. Monitoring

Pada tahapan monitoring penulis akan melakukan pemantauan terhadap kinerja sistem yang telah diimplementasikan pada jaringan. Tujuan dari tahapan ini agar penulis dapat melihat efektivitas dari kinerja sistem apakah sudah berjalan sesuai dengan yang diharapkan dan tercapainya tujuan awal dari pembuatan sistem autentikasi dengan *single sign-on* ini.

2.6. Manajemen

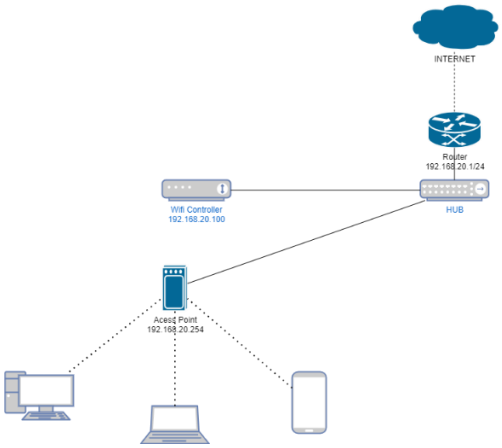
Pada tahapan manajemen sistem akan diberikan sebuah rules. *Rules* yang akan diberikan seperti pada *firewall Windows server* agar *database* dapat terhubung ke perangkat jaringan. Pemberian *rules* pada tahapan manajemen berguna untuk menjaga unsur *reliability* pada sistem yang telah diterapkan.

3. HASIL DAN PEMBAHASAN

Sistem autentikasi ini diperuntungkan untuk user ketika ingin terhubung kedalam jaringan. Fokus dari pembuatan sistem ini adalah memberikan kenyamanan serta keamanan yang lebih terjaga ketika user ingin terhubung kedalam jaringan.

3.1. Analisis

Analisis dilakukan pada sistem lama yang merupakan sebuah proses untuk memahami serta mengidentifikasi sistem yang berjalan dan memiliki tujuan untuk mengumpulkan informasi mengenai kekurangan pada sistem tersebut. Selaras dengan tujuannya, analisis pada sistem lama akan berguna untuk memberikan solusi dalam mengatasi permasalahan pada sistem yang telah berjalan. Sistem autentikasi *user* yang berjalan pada saat ini dideskripsikan seperti yang ada pada Gambar 1 berikut.

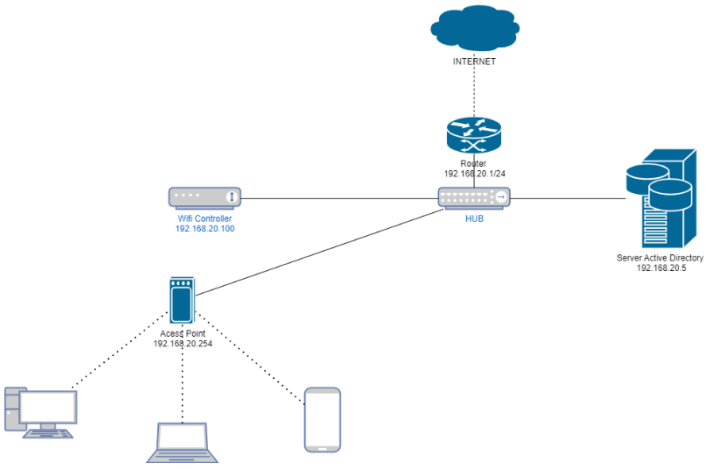


Gambar 1. Topologi sistem yang berjalan

3.2. Desain rancangan sistem

Desain dilakukan untuk memberikan deskripsi dari rancangan sistem autentikasi *user* yang akan di terapakan nantinya. Pada tahapan desain ini, diberikan gambaran rancangan sistem dengan menggunakan rancangan topologi. Pemilihan gambaran topologi akan berguna sebagai media untuk memberikan deskripsi rancangan sistem, alasannya adalah gambaran topologi ini memuat

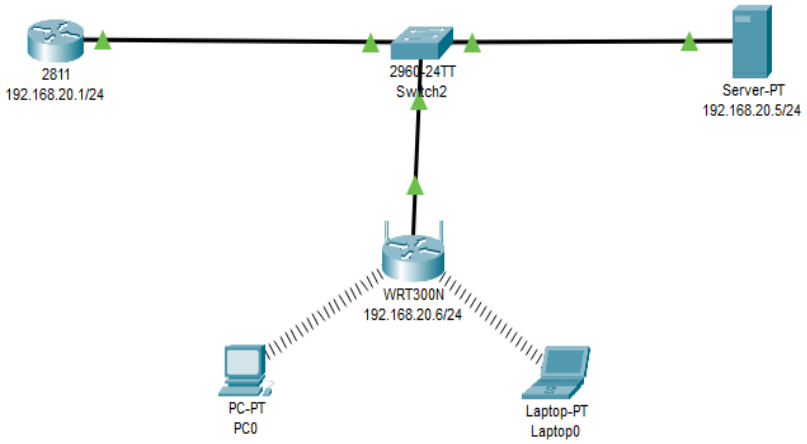
setiap alur yang dimulai dari *user* hingga ke sistem autentikasi *use*r dan tergambarkan secara terstruktur. Desain dari rancangan sistem dapat dilihat pada Gambar 2 berikut.



Gambar 2. Topologi sistem yang diusulkan

3.3. Simulasi

Simulasi pada tahapan ini diperlukan untuk menguji kinerja dari alur proses berjalannya sistem yang akan diimplementasikan. Pada tahapan simulasi berikut pengujian dilakukan menggunakan aplikasi *cisco packet tracer*. Simulasi berikut terdapat 5 perangkat yang masuk ke dalam rancangan skala jaringan, yaitu *server*, *router*, *wireless access point*, laptop, dan PC seperti tampak pada Gambar 3. Pada simulasi berikut cakupan jaringan yang digunakan adalah LAN atau biasa dikenal *Local Area Network*. Pemilihan jaringan *local area network* dilakukan karena implementasi sistem akan dilakukan pada jaringan yang berada di dalam gedung. Pada Gambar 3 terdapat tampilan dari rancangan sistem yang di simulasikan melalui aplikasi *cisco packet tracert.*



Gambar 3. Cakupan jaringan pada simulasi

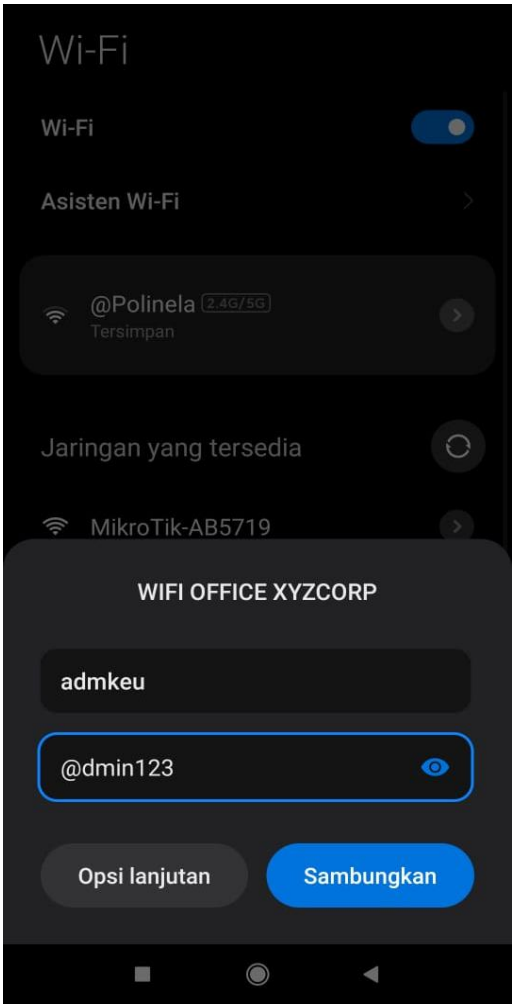
3.4. Implementasi

Implementasi sistem dilakukan untuk menerapkan rancangan yang telah dibuat agar dapat mewujudkan hasil yang di harapkan. Pada tahapan implementasi penerapan sistem yang telah di

rancang akan dijalankan dan digunakan oleh *user*. Berikut di bawah ini adalah proses dari autentikasi *user* menggunakan metode *single sign-on* berbasis *windows active directory*.

1. Perangkat *user* tanpa *join domain*

   Perangkat *user* seperti *mobile device* yang belum terkoneksi ke dalam jaringan *wireless a*kan menampilakan halaman untuk *login* terlebih dahulu. *Login* pada jaringan akan menggunakan akun yang ada pada *database active directory* hal ini dapat dilihat seperti yang ada pada Gambar 4.



Gambar 4. Proses login

2. Perangkat *user* dengan *join domain*

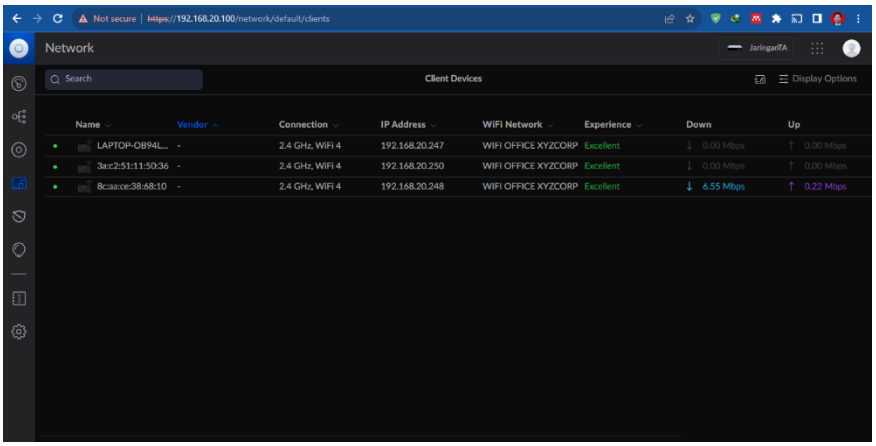
   Pada perangkat *user* yang telah melakukan join domain ke *server active directory* proses untuk terhubung ke dalam jaringan akan berbeda. Setelah bergabung dengan domain menggunakan akun yang terdaftar di *active directory*, perangkat tersebut dapat terhubung ke dalam jaringan dengan lebih mudah, seringkali hanya dengan menekan tombol *connect*. Hal ini dimungkinkan berkat adanya layanan *active directory certificate* yang terintegrasi dengan *active directory*. Layanan ini memungkinkan penerbitan dan manajemen sertifikat digital. Ketika perangkat telah memenuhi syarat-syarat tertentu untuk bergabung ke dalam jaringan, layanan *active directory certificate* akan secara otomatis melaksanakan proses pemberian sertifikat (*enrollment*). Pada Gambar 5 dibawah ini terdapat tampilan proses *login* dari perangkat yang telah melakukan *join domain*, seperti yang terlihat *user* tidak perlu

lagi memasukan informasi mengenai *username* dan password hanya perlu menekan tombol *connect* agar dapat terhubung kedalam jaringan.

Gambar 5. Proses login

3.5. Monitoring

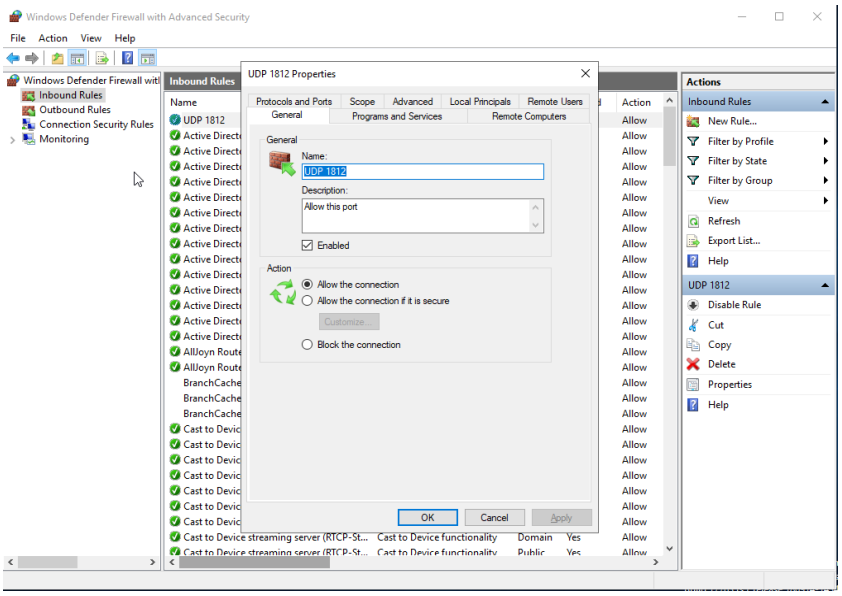
Pada tahapan ini monitoring akan dilakukan pada perangkat yang terhubung ke dalam jaringan. Hal ini dilakukan untuk memastikan sistem autentikasi *user* dengan metode *single sign-on* berbasis *Windows active directory* pada PT. XYZ berjalan serta berfungsi sesuai dengan tujuannya. Monitoring dilakukan dengan mengecek informasi kecepatan internet yang perangkat dapatkan, IP addres yang diberikan, serta informasi lain yang berhubungan dengan penggunaan jaringan *wireless*. Monitoring pada perangkat yang terhubung dapat dilakukan melalui unifi *controller* seperti yang ada pada Gambar 6 berikut.



Gambar 6. Monitoring perangkat

3.6. Manajemen *rules firewall* pada *server*

Manajemen *rules firewall* dilakukan pada *server Windows*. Manajemen yang dilakukan dengan memberikan *rules inbound* pada *firewall* di *Windows server*. *Rules* tersebut akan mengizinkan *port* 1812 untuk masuk dan terhubung kedalam perangkat *server*. Hal ini bertujuan untuk komunikasi dengan wifi *controller*, pada perangkat wifi *controller* agar dapat berkomunikasi dan terhubung ke *Windows active directory* dengan layanan RADIUS maka diperlukan akses untuk *port* 1812 yang merupakan *port default* RADIUS *profile* di wifi *controller*. Berikut di bawah ini adalah Gambar 7 yang merupakan tampilan dari *firewall windows server*.



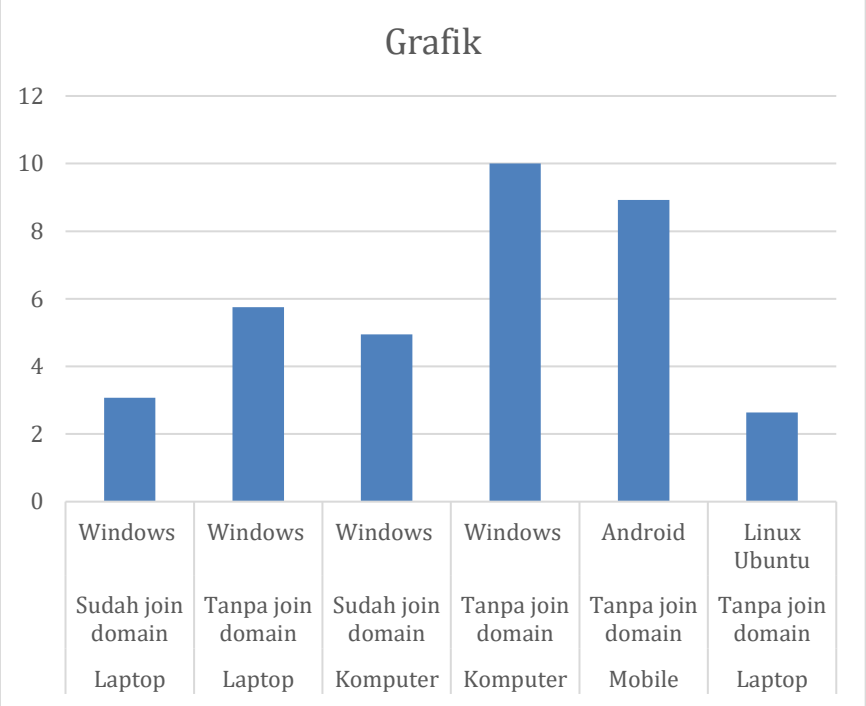
Gambar 7. Rules firewall windows server

3.7. Observasi sistem autentikasi *single sign-on*

Observasi dilakukan terhadap lama waktu perangkat terhubung ke dalam jaringan dengan menggunakan autentikasi single sign-on. Objek pengamatan observasi adalah perangkat seperti laptop, komputer, dan mobile. Data dari hasil observasi akan berguna sebagai bahan untuk peninjauan kinerja sistem autentikasi yang berjalan. Berikut Tabel 1 dan Gambar 8 yang berisi informasi mengenai durasi waktu yang dibutuhkan pada masing – masing perangkat dengan sistem operasi yang berbeda agar dapat terhubung ke dalam jaringan menggunakan metode autentikasi *single sign-on*.

Tabel 1. Observasi waktu terkoneksi ke dalam jaringan

No	Perangkat	Status Perangkat	Sistem Operasi	Durasi Waktu (Detik)
1	Laptop	Sudah join domain	Windows	3,07
2	Laptop	Tanpa join domain	Windows	5,75
3	Komputer	Sudah join domain	Windows	4,95
4	Komputer	Tanpa join domain	Windows	10
5	Mobile	Tanpa join domain	Android	8,92
6	Laptop	Tanpa join domain	Linux Ubuntu	2,64
Rata - rata				5,89



Gambar 8. Grafik observasi

Berdasarkan informasi yang didapatkan dari hasil observasi yang dilakukan, dapat diambil sebuah kesimpulan. Kesimpulan tersebut adalah rata – rata waktu yang didapatkan dari seluruh perangkat yang menjadi objek pengamatan untuk terhubung ke dalam jaringan menggunaan autentikasi user dengan metode single sign-on adalah 5,89 detik.

4. KESIMPULAN

Kesimpulan yang dapat diberikan adalah telah dihasilkan sistem autentikasi *user* dengan metode *single sign-on* berbasis *windows active directory* pada PT. XYZ. Dengan adanya sistem autentikasi ini dapat memberikan keuntungan dalam segi keamanan serta kemudahan bagi user ketika ingin terhubung kedalam jaringan. Autentikasi menggunakan WPA2 - Enterprise akan mengharuskan user untuk masuk menggunakan username dan password dari sebuah akun, akun tersebut sama seperti email serta aplikasi perusahaan. 2. Dengan WPA2 - Enterprise akses untuk masuk ke dalam jaringan akan terbatas. Perangkat yang tidak memasukan username dan password atau tidak melakukan join domain dengan akun yang ada di active directory dipastikan tidak dapat mengakses jaringan *wireless* serta mendapatkan IP address dari DHCP server. Beberapa potensi pengembangan dapat dilakukan dengan menambahkan teknologi kecerdasan buatan. AI dapat memantau pola perilaku pengguna, seperti cara mereka mengetik, berjalan, atau menggunakan perangkat, untuk autentikasi. Teknologi ini dapat membantu mendeteksi anomali dalam perilaku yang mungkin menunjukkan upaya akses yang tidak sah[11], [12].

DAFTAR PUSTAKA

[1] E. A. Darmadi, "PERANCANGAN SISTEM OTENTIKASI RADIUS PADA PENGGUNA JARINGAN WIRELESS UNTUK MENINGKATKAN KEAMANAN JARINGAN KOMPUTER," *IKRA-ITH Inform. J. Komput. Dan Inform.*, vol. 2, no. 3, Art. no. 3, Nov. 2018.
[2] A. Darmadi, "Perancangan Sistem Otentikasi Radius Pada Pengguna Jaringan Wireless Untuk Meningkatkan Keamanan Jaringan Komputer," vol. 2, no. 3, pp. 9–16, 2018.
[3] S. D. Putra, A. S. Ahmad, and S. Sutikno, "DPA-countermeasure with knowledge growing system," in *2016 International Symposium on Electronics and Smart Devices (ISESD)*, Bandung, Indonesia: IEEE, Nov. 2016, pp. 16–20. doi: 10.1109/ISESD.2016.7886757.
[4] S. D. Putra, S. Sutikno, Y. Rosmansyah, and I. Asrowardi, "Integrated implementation of service and information security management system," in *2014 International Conference on ICT For Smart Society (ICISS)*, Bandung, Indonesia: IEEE, Sep. 2014, pp. 185–191. doi: 10.1109/ICTSS.2014.7013171.
[5] S. D. Putra, A. D. W. Sumari, I. Asrowardi, E. Subyantoro, and L. M. Zagi, "First-Round and Last-Round Power Analysis Attack Against AES Devices," in *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung, Indonesia: IEEE, Oct. 2020, pp. 410–415. doi: 10.1109/ICITSI50517.2020.9264976.
[6] S. D. Putra, A. D. W. Sumari, I. Asrowardi, E. Subyantoro, and L. M. Zagi, "First-round and last-round power analysis attack against AES devices," *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020 - Proceedings*. pp. 410–415, 2020. doi: 10.1109/ICITSI50517.2020.9264976.
[7] S. D. Putra, A. D. W. Sumari, I. Asrowardi, and E. Subyantoro, "Power Analysis in Hamming Weight Model: Attacking IoT Encryption Devices," in *2021 4th International Conference on Signal Processing and Information Security (ICSPIS)*, Dubai, United Arab Emirates: IEEE, Nov. 2021, pp. 41–44. doi: 10.1109/ICSPIS53734.2021.9652185.
[8] M. E. Ahmed, "DDoS attack mitigation in internet of things using software defined networking," *Proceedings - 3rd IEEE International Conference on Big Data Computing Service and Applications, BigDataService 2017*. pp. 271–276, 2017. doi: 10.1109/BigDataService.2017.41.
[9] V. Rao, "Light-weight hashing method for user authentication in Internet-of-Things," *Ad Hoc Networks*, vol. 89. pp. 97–106, 2019. doi: 10.1016/j.adhoc.2019.03.003.
[10] T. Sanjaya and D. Setiyadi, "Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim," *Mhs. Bina Insani*, vol. 4, no. 1, pp. 1–10, 2019.
[11] F. Wijitrisnanto, S. Sutikno, and S. D. Putra, "Efficient Machine Learning Model for Hardware Trojan Detection on Register Transfer Level," in *2021 4th International Conference on Signal Processing and Information Security (ICSPIS)*, Dubai, United Arab Emirates: IEEE, Nov. 2021, pp. 37–40. doi: 10.1109/ICSPIS53734.2021.9652443.
[12] S. Sutikno, S. D. Putra, F. Wijitrisnanto, and M. E. Aminanto, "Detecting Unknown Hardware Trojans in Register Transfer Level Leveraging Verilog Conditional Branching Features," *IEEE Access*, vol. 11. pp. 46073–46083, 2023. doi: 10.1109/ACCESS.2023.3272034.