JOINT (*Journal of Information Technology*) (p)ISSN: 2527-9467/(e)ISSN: 2656-7539
Vol. 02 No 01 Februari 2020, pp. 17-24

Analisis dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication

Muchamad Rusdan[1], Muhamad Sabar[2]

[1,2]*Teknik Informatika, Sekolah Tinggi Teknologi Bandung*

[1]rusdan@sttbandung.ac.id

[2]sabar@sttbandung.ac.id

Intisari—**Jaringan wireless merupakan salah satu alternatif terbaik dalam membangun jaringan komputer yang praktis dan fleksibel serta memiliki mobilitas tinggi. Sebagian besar institusi menggunakan jaringan wireless untuk mendukung jaringan kabel yang sudah ada, namun pada kenyataannya jaringan wireless tersebut tetap menggunakan media kabel sebagai backbone dari access point, yang bertujuan supaya pengguna layanan bisa melakukan akses internet dan pencarian informasi. Permasalahan dari penggunaan kabel sebagai media backbone ini dapat menjadi kendala yang berarti pada tempat-tempat yang sulit dijangkau oleh kabel. Jaringan wireless memberikan kemudahan dan fleksibilitas yang cukup tinggi serta nyaman untuk digunakan. Selama berada dalam area cakupan jaringan wireless, pengguna dapat mengakses internet setiap saat. Untuk membuat sebuah jaringan wireless terkoneksi ke internet dengan aman dan user-friendly, maka kita dapat membuat sebuah sistem user authentication yang berbasis Multi-Factor Authentication (MFA) yang dapat digunakan untuk melakukan Authentication dan Authorization. Pada umumnya setiap pengguna dapat menggunakan layanan jaringan wireless yang ada dengan cara melakukan user authentication yang berbasis Wifi Protected Access 2 Pre-Shared Key (WPA2-PSK). Tujuan penelitian ini antara lain adalah mengembangkan jaringan wireless yang menggunakan user authentication berbasis Multi-factor Authentication (MFA) untuk dapat melakukan koneksi pada jaringan wireless demi meningkatkan keamanan serta kemudahan dalam penggunaan jaringan wireless yang ada. Metode penelitian yang digunakan pada penelitian ini menggunakan metode penelitian deskriptif kualitatif, dengan pengumpulan data menggunakan teknik studi literatur dan observasi. Setelah dilakukan analisis dan disain dapat disimpulkan bahwa user authentication berbasis Multi-factor Authentication (MFA) aman dan user-friendly yang mampu membedakan pengguna yang diizinkan dan tidak diizinkan untuk menggunakan layanan jaringan wireless.**

Kata kunci— **jaringan wireless, wireless distribution system, multi-factor authentication.**

Abstract— **Wireless networks are one of the best alternatives in building practical and flexible computer networks that have high mobility. Most of them use wireless networks to support existing cable networks, but on wireless networks, they still use cable media as a backbone of the access point, which supports communication users can access the internet and find information. The problem of using cables as backbone media can be a significant challenge in places that are difficult to reach by wires. Wireless networks provide convenience and convenience that is high enough to use. As long as they are in an area that is supported by a wireless network, users can access the internet at any time. To make the wireless network connected to the internet safe and easy to use, we can create a user authentication system based on Multi-Factor Authentication (MFA) that can be used to authenticate and authorize. In general, each user can use existing wireless network services by verifying users based on Wifi Protected Access 2 Pre-Shared Key (WPA2-PSK). The purpose of this research is to develop a wireless network that uses Multi-Factor Authentication (MFA) based user authentication to be able to connect to the wireless network to increase security and provide the use of existing wireless networks. The research method used in this study uses descriptive qualitative research methods, with data collection using literature study and observation techniques. After analysis and design, it can be concluded that user authentication is based on Multi-factor Authentication (MFA) in a safe and user-friendly manner that can determine the users who are allowed and not allowed to use wireless networks.**

Keywords— ***wireless network, wireless distribution system, multi-factor authentication*.**

I. PENDAHULUAN

Internet telah merubah banyak hal, khususnya didalam pemenuhan kebutuhan akan informasi dan sistem jaringan yang luas menciptakan banyak kemudahan akses informasi tidak lagi hanya terhubung ke *internet*, namun juga sudah mulai bergeser pada kemampuan mobilitas pengguna yang selalu terhubung dengan *internet* dengan cepat bahkan *realtime*[1]. Untuk memenuhi sifat mobilitas dan selalu terhubung dibutuhkan solusi jaringan *wireless*. Jaringan *wireless* adalah salah satu teknologi yang saat ini sudah digunakan secara luas diberbagai institusi, bandara, hotel, dan sekolah[2].

Jaringan *wireless* merupakan salah satu alternatif terbaik dalam membangun jaringan komputer yang praktis dan fleksibel serta memiliki mobilitas tinggi. Sebagian besar institusi menggunakan jaringan wireless untuk mendukung jaringan kabel yang sudah ada, namun pada kenyataannya jaringan *wireless* tersebut tetap menggunakan media kabel sebagai *backbone* dari *access point*, yang bertujuan supaya pengguna layanan bisa melakukan akses internet dan pencarian informasi[3]. Permasalahan dari penggunaan kabel

sebagai media backbone ini dapat menjadi kendala yang berarti pada tempat-tempat yang sulit dijangkau oleh kabel. Salah satu alternatif solusi dari masalah tersebut adalah dengan menerapkan *Wireless Distribution System* (WDS). WDS merupakan salah satu sistem dan/atau mode untuk mengembangkan jaringan *wireless* tanpa harus menggunakan kabel sebagai *backbone* dari *access point* melainkan memanfaatkan jalur sinyal wireless dari access point tersebut[4].

Jaringan *wireless* saat ini menjadi salah satu fasilitas standar yang diberikan kepada pengguna yang dapat diakses melalui *laptop, smartphone, tablet,* dan perangkat lainnya yang mendukung jaringan *wireless*. Fasilitas tersebut banyak membantu pengguna dalam proses pencarian informasi[5]. Jaringan *wireless* yang ada pada umumnya masih mempergunakan kabel *Unshielded Twisted Pair* (UTP) sebagai *backbone* dari *access point*. Penggunaan kabel UTP sebagai *backbone* dari *access point* menjadi salah satu kendala yang dihadapi jika area cakupan yang harus terlayani akses jaringan wireless sangat luas, karena dengan backbone yang menggunakan kabel UTP memiliki keterbatasan jarak, semakin jauh jarak yang ditempuh maka semakin banyak kabel UTP yang harus digunakan dan akan sangat berpengaruh pada pengiriman dan penerimaan arus data.

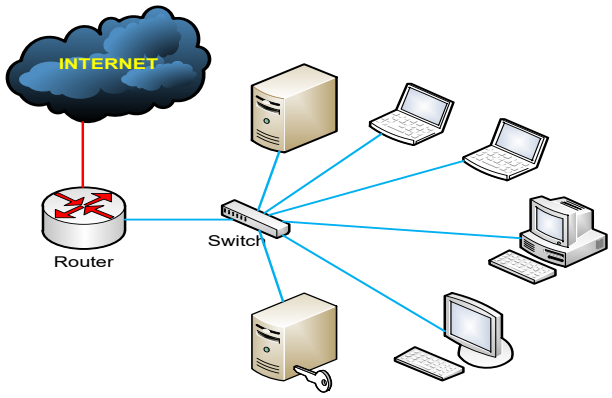
Jaringan *wireless* memberikan kemudahan dan fleksibilitas yang cukup tinggi serta nyaman untuk digunakan. Selama berada dalam area cakupan jaringan *wireless*, pengguna dapat mengakses *internet* setiap saat[6]. Untuk membuat sebuah jaringan *wireless* terkoneksi ke internet dengan aman dan *user-friendly*, maka kita dapat membuat sebuah sistem *user authentication* yang berbasis *Multi-Factor Authentication* (MFA) yang dapat digunakan untuk melakukan *Authentication* dan *Authorization*. Pada umumnya setiap pengguna dapat menggunakan layanan jaringan *wireless* yang ada dengan cara melakukan user authentication yang berbasis *Wifi Protected Access 2 Pre-Shared Key* (WPA2-PSK). Sehingga sangat sulit untuk membedakan pengguna yang diijinkan dan tidak diijinkan untuk menggunakan layanan jaringan *wireless* tersebut dan penggunaan WPA2-PSK dianggap tidak aman untuk jaringan *wireless public*[7].

Tujuan penelitian ini antara lain adalah mengembangkan jaringan *wireless* yang menggunakan *user authentication* berbasis *Multi-factor Authentication* (MFA) untuk dapat melakukan koneksi pada jaringan *wireless* demi meningkatkan keamanan serta kemudahan dalam penggunaan jaringan *wireless* yang ada.

II. LANDASAN TEORI

A. *Jaringan Komputer*

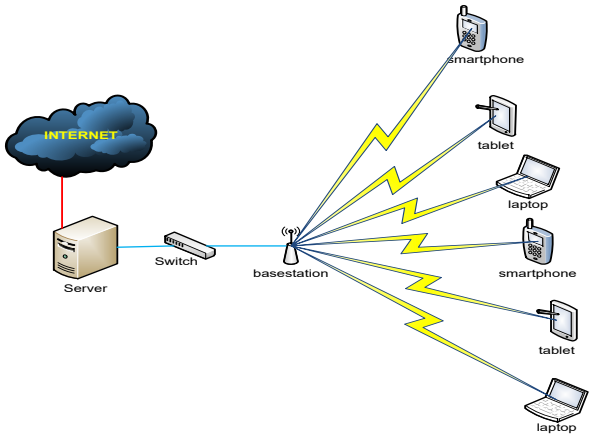
Jaringan Komputer merupakan suatu kumpulan komputer yang terdiri dari dua atau lebih jumlah komputer, yang masing-masing berdiri sendiri dan terhubung melalui suatu media komunikasi[8]. Media yang menghubungkan komputer tidak hanya melalui kabel tembaga saja, melainkan dapat juga melalui fiber optic, gelombang radio, *infrared*, dan satelit[9]. Kecepatan transfer dari suatu jaringan sering disebut sebagai bandwidth, satuan yang dipakai dalam mengukur bandwidth ini dapat berupa bit per-detik ataupun byte per-detik[10]. Satu byte terdiri dari 8 bit data. Sedangkan 1 kilobyte data terdiri dari 1024 byte data.



Gambar 1. Jaringan Komputer

B. *Jaringan Wireless*

Jaringan *wireless* merupakan suatu jaringan yang tidak menggunakan media kabel tapi menggunakan pancaran gelombang radio untuk interaksi atau komunikasi antar perangkat yang mendukung koneksi *wireless*[11]. Bekerja pada frekuensi 2,4 GHz (802.11 b/g/n/ac) atau 5 GHz (802.11 a/n/ac). *Backbone* jaringan *wireless* biasanya menggunakan kabel, dengan satu atau lebih titik akses[11].



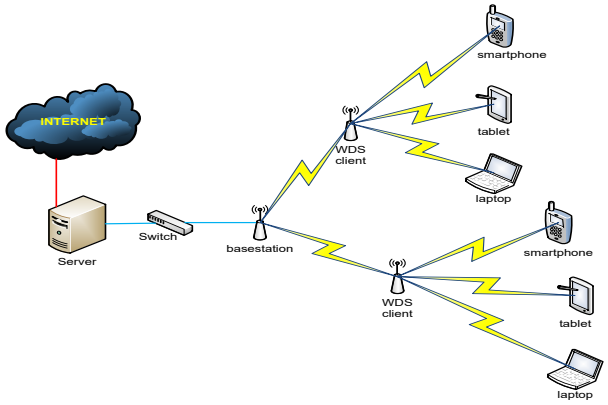
Gambar 2. Jaringan *Wireless*

C. *Wireless Distribution System (WDS)*

Wireless Distribution System merupakan koneksi yang memungkinkan interkoneksi antar *access point* (AP) sehingga pengguna dapat "*roaming*" antar *Base Station*[12]. *Wireless Distribution* System adalah jaringan *wireless* yang mencakup area yang lebih luas dan *Wireless Distribution System* juga merupakan kumpulan dari LAN *wireless*[12].

Wireless Distribution System memungkinkan jaringan *wireless* dikembangkan menggunakan beberapa *access point* tanpa harus memerlukan *backbone* kabel jaringan untuk menghubungkanya[12]. Keuntungan yang bisa terlihat dari *Wireless Distribution System* dibanding solusi lainnya adalah bahwa dengan *Wireless Distribution System*, *header Media Access Control* (MAC) *Address* dari paket *traffic* tidak berubah antar *link access point*. Pada jaringan wireless dengan menggunakan *mode* WDS *bridge*, komunikasi dua arah antara access point yang satu dengan *access point*

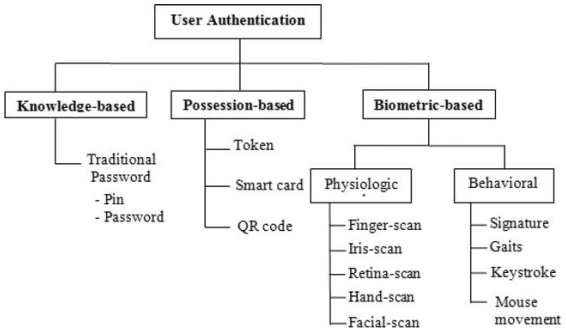
lainnya tidak membolehkan *wireless clients* atau *station* untuk mengaksesnya[12].



Gambar 3. *Wireless Distribution System*

D. *User Authentication*

User authentication merupakan bagian dari otentikasi entitas atau identifikasi, yang merupakan pembuktian terhadap identitas suatu entitas, bisa berupa orang, kartu kredit atau mesin[13].



Gambar 4. *User Authentication*[13]

User authentication dilakukan untuk memastikan siapa pengguna jaringan sebenarnya. Hal ini untuk mencegah seseorang yang tidak diharapkan dapat mengakses suatu jaringan. *User Authentication* mengidentifikasi pengguna jaringan dengan menggunakan *nama pengguna* dan *kata sandi* yang dimasukkan oleh pengguna ke dalam sistem[13].

Gambar 5. *User Authentication Konsep User Authentication*[13]

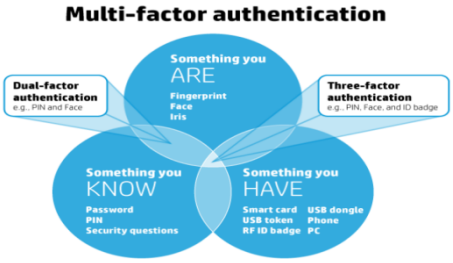
Authentication seringkali diasumsikan identik dengan otorisasi, banyak protokol keamanan, dan peraturan yang berdasarkan asumsi ini. Akan tetapi, penggunaan istilah autentikasi yang lebih tepat adalah pembuktian sebagai proses pengecekan identitas seorang pengguna, sedangkan autorisasi adalah proses pengecekan bahwa pengguna yang dikenal memiliki kekuasaan untuk melakukan tindakan tertentu[13].

User Authentication adalah proses usaha pengecekan identitas seorang pengguna sistem komunikasi pada proses *login* ke dalam sebuah sistem. Pengguna yang telah lolos pengecekan identitas adalah pengguna resmi pada sistem, orang yang memiliki otoritas atas sistem, atau mungkin aplikasi yang berjalan pada sistem. Penggunaan sistem *authentication* diharapkan dapat membentuk sebuah sistem khusus, yang hanya dapat dipergunakan oleh orang-orang yang memiliki hak guna.

Gambar 6. *Evolusi Metode Authentication Dari SFA Ke MFA (Alizadeh, Hassan, & Khodadadi, 2015)*

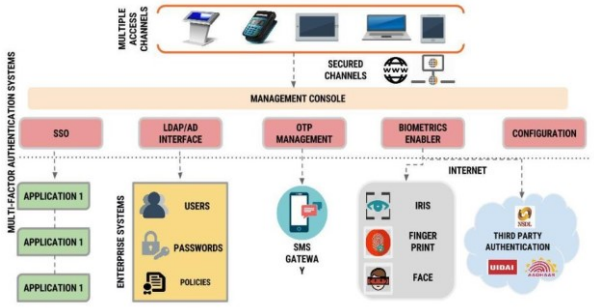
E. *Multi-Factor Authentication*

Multi-factor authentication (MFA) adalah sistem keamanan yang menggunakan lebih dari satu metode *authentication* dari kategori *independent credentials* untuk memverifikasi identitas pengguna untuk dapat login atau melakukan transaksi lainnya[14].



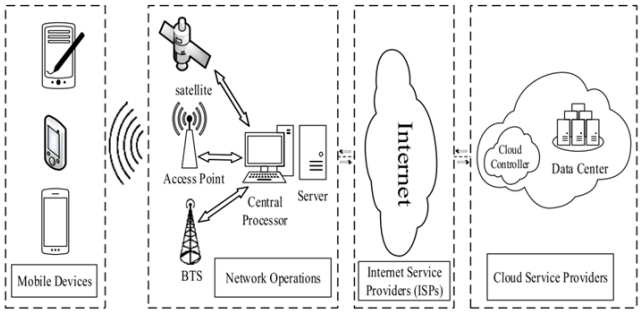
Gambar 7. Konsep *Multi-Factor Authentication*[14]

Multi-factor authentication menggabungkan dua atau lebih *independent credentials* apa yang diketahui pengguna (*kata sandi*), apa yang dimiliki pengguna (*security token*), dan siapa penggunanya (*biometric verification*). Tujuan dari MFA adalah untuk menciptakan pertahanan berlapis dan membuatnya lebih sulit bagi orang yang tidak sah untuk mengakses target seperti lokasi fisik, perangkat komputasi, jaringan atau basis data[14]. Jika salah satu faktor dikompromikan atau rusak, penyerang masih memiliki setidaknya satu lagi penghalang untuk dilanggar sebelum berhasil membobol target.



Gambar 8. Sistem Kerja *Multi-Factor Authentication*

Pada penelitian Alizadeh, Hassan, dan Khodadadi untuk melindungi informasi rahasia pengguna pada *mobile cloud computing*, data harus dapat diakses oleh orang yang berhak dengan menggunakan lebih dari satu faktor otentikasi atau *multi-factor authentication* (MFA). MFA menawarkan keamanan dan privasi yang lebih baik. MFA adalah salah satu metode yang paling cocok untuk diterapkan pada *mobile cloud computing*[13].



Gambar 9. *Mobile Cloud Computing Architecture* (Alizadeh, Hassan, & Khodadadi, 2015)

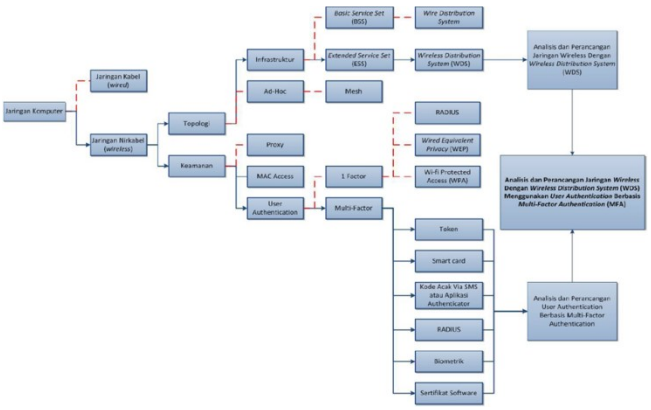
Pada penelitian Ometov, Bezzateev, Mäkitalo, Andreev, Mikkonen, dan Koucheryavy (2018), menjelaskan bahwa pada saat ini *authentication* lebih penting daripada sebelumnya. Sebagian besar pengguna akan bergantung pada biometrik dalam hal-hal yang menyangkut keamanan sistem dan otorisasi untuk melengkapi *kata sandi* konvensional. Meskipun privasi, keamanan, kegunaan, dan masalah akurasi masih ada, MFA menjadi sebuah sistem yang menjanjikan keamanan dan kemudahan penggunaan yang diperlukan untuk pengguna modern dalam memperoleh akses ke data sensitif. Biometrik merupakan salah satu lapisan kunci untuk memungkinkan masa depan MFA[15].

Gambar 10. Konsep *Multi-Factor Authentication*

Pada penelitian Nwabueze, Obioha, dan Onuoha (2017), menyimpulkan bahwa *multi-factor authentication* yang ditingkatkan memastikan keamanan informasi untuk perusahaan bisnis dan mencegahnya agar tidak macet atau kehilangan uang. *multi-factor authentication* yang ditingkatkan memberikan validasi pengguna yang hemat biaya, fleksibel, nyaman, dan tidak memiliki kerumitan untuk pekerja jarak jauh (remotely). Selain itu, dapat melibatkan penggunaan strategi keamanan yang lengkap untuk melindungi data penting dari pelaku kejahatan (Nwabueze, Obioha, & Onuoha, 2017).

F. Kerangka Pemikiran

Pada bagian ini akan gambarkan bagaimana kerangka pemikiran dari penelitian ini. Seperti dapat dilihat pada gambar 11.



Gambar 11. Kerangka Pemikiran

III. METODE PENELITIAN

A. Metode Penelitian

Metode penelitian yang digunakan pada penelitian ini menggunakan metode penelitian deskriptif kualitatif, dengan pengumpulan data menggunakan teknik studi literatur dan observasi.

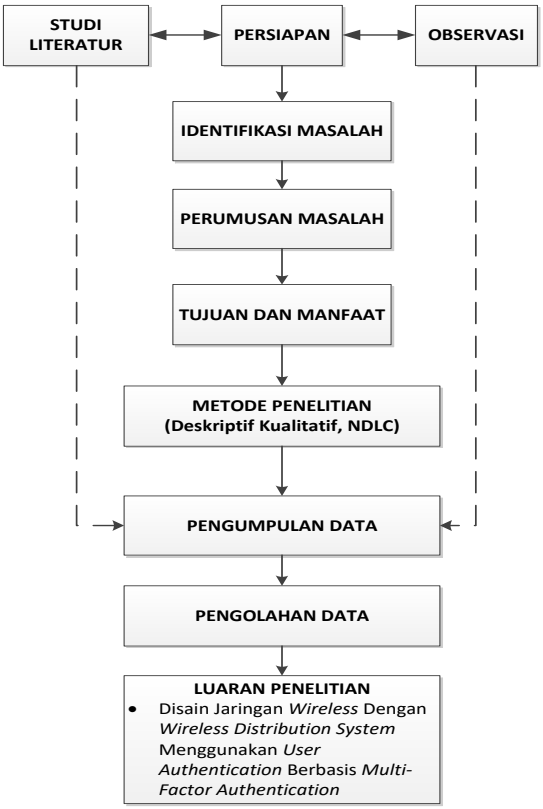
Menurut Sugiyono (2010), menjelaskan bahwa teknik studi literatur dilakukan dengan cara mempelajari literatur-literatur yang ada hubungannya dengan objek penelitian. Pada penelitian ini, teknik pengumpulan data berhubungan dengan topik yang diangkat dalam penelitian ini[16]. data didapatkan dari berbagai sumber buku, majalah, jurnal, tesis, disertasi, dan *internet*. Sedangkan teknik observasi merupakan teknik pengumpulan data melalui pengamatan langsung dan/atau peninjauan secara cermat dan langsung di lapangan atau lokasi penelitian16].

B. Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan pada penelitian ini yaitu metode *Network Development Life Cycle* (NDLC) yang tahapannya dapat dijelaskan sebagai berikut:

1. Analisis, tahap awal ini dilakukan analisis kebutuhan, analisis permasalahan yang muncul, analisis keinginan *pengguna*, dan analisis topologi jaringan yang sudah ada saat ini.
2. Disain, tahap desain ini akan menghasilkan desain topologi jaringan *wireless* yang akan dibangun dan/atau dikembangkan, diharapkan dengan desain akan memberikan gambaran seutuhnya dari kebutuhan yang ada.
3. *Prototype*, tahap ini yang akan diterapkan adalah membuat *prototype* dalam skala yang kecil dan/atau tahap uji coba pada jaringan *wireless* dari titik *basestation point* ke *access point* pada tiap gedung yang ada.

C. Diagram Alir Penelitian



Gambar 12. Diagram Alir Penelitian

IV. HASIL DAN PEMBAHASAN

Keseluruhan proses *authentication* untuk *Multi-factor Authentication* (MFA) memerlukan setidaknya dua dari tiga metode *authentication* yang dapat dijelaskan sebagai berikut[17]:

1. *Something you know*, seperti kata sandi, PIN, atau jawaban dari pertanyaan rahasia.
2. *Something you have*, seperti perangkat *token* atau *smartcard*, *token* keamanan fisik atau *logic*, *one-time password* (OTP) *token*, kartu akses karyawan, dan kartu SIM ponsel.
3. *Something you are*, seperti biometrik yang terdiri dari *scan* retina, *scan* iris, *scan* sidik jari, *scan* pembuluh darah jari, *recognition* wajah, *recognition* suara, dan geometri tangan.

Geolocation dan waktu dapat dijadikan sebagai informasi lain yang dapat ditambahkan ke dalam proses *authentication.* Data *geolocation* dan waktu dapat digunakan untuk membatasi akses *remote* seseorang ke dalam jaringan dan dapat mengurangi risiko pembajakan akun serta aktivitas jahat lainnya.

Mekanisme *authentication* yang digunakan untuk MFA harus bersifat independen satu sama lain sehingga akses ke satu faktor tidak memberikan akses ke faktor lain, dan kompromi dari satu faktor tidak memengaruhi integritas atau kerahasiaan faktor lainnya.

A. Skenario Authentication Umum MFA

Menurut PCI Security Standards Council (2017), menjelaskan bahwa dalam menerapkan *multi-factor authentication* terdapat 4 skenario yang dapat dijadian acuan atau standar dalam membangun MFA. Skenario tersebut dapat dijelaskan sebagai berikut[17]:

1. Skenario 1

Gambar 13. Skenario *Authentication* Umum MFA 1

Pengguna menggunakan *kata sandi* A untuk masuk ke suatu perangkat dan juga untuk mengakses *token* yang tersimpan pada perangkat. Lalu kemudian membuat koneksi ke jaringan perusahaan, dengan menggunakan *kata sandi* B yang berbeda dan *one-time password* (OTP) yang dihasilkan oleh *token* perangkat lunak sebagai *authentication*. Selanjutnya sistem akan memberikan akses yang diminta oleh *pengguna* jika kedua faktor yang diberikan valid.

2. Skenario 2

Gambar 14. Skenario *Authentication* Umum MFA 2

Pada skenario 2, *pengguna* menggunakan kata sandi A atau salah satu biometrik untuk dapat masuk ke dalam perangkat. selanjutnya menyediakan akses ke token perangkat lunak yang tersimpan di perangkat. Untuk kemudian dapat memulai koneksi ke jaringan perusahaan, sebelumnya *pengguna* menjalankan *web browser* yang terlebih dahulu telah diisi *credential* yang tersimpan pada perangkat.

3. Skenario 3

Gambar 15. Skenario *Authentication* Umum MFA 3

Pada Skenario 3, *pengguna* menggunakan *nama pengguna* dan *kata sandi* untuk masuk ke perangkat. Koneksi ke jaringan perusahaan membutuhkan set kredensial awal dan OTP yang dihasilkan oleh *software token* yang berada pada perangkat seluler.

4. Skenario 4

Gambar 16. Skenario *Authentication* Umum MFA 3

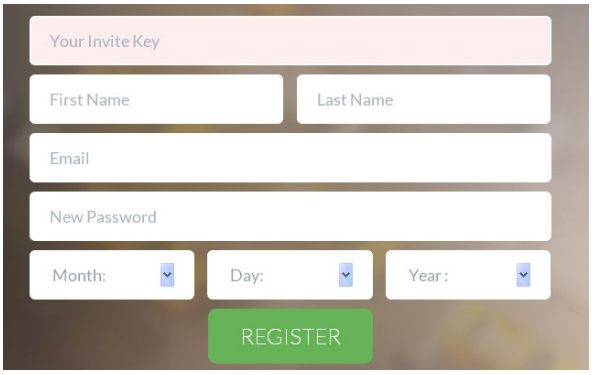
Pada skenario 4, *pengguna* menggunakan *kata sandi* dan biometrik untuk masuk ke perangkat. Untuk membuat koneksi ke jaringan perusahaan, kemudian pengguna memberikan *signature* seperti kata sandi yang berbeda, sertifikat digital, atau respons tantangan yang ditandatangani.

B. Disain Sistem Yang Diusulkan

Pemanfaatan infrastruktur jaringan yang telah ada dapat mengurangi biaya yang harus dikeluarkan untuk sistem yang diusulkan. Pada setiap sistem pemrosesan *authentication*, *identity*, *integrity*, *confidentiality*, *non-repudiation,* dan *authenticity* menjadi sesuatu yang sangat penting. Pada peningkatan keamanan proses MFA dengan mengirimkan *one-time password* (OTP) hanya kepada *pengguna* tepercaya yang memiliki hak akses. Disain sistem yang diusulkan memiliki beberapa tahapan dalam melakukan proses MFA, tahapan tersebut dalam dijelaskan sebagai berikut:

1. Tahap Pendaftaran

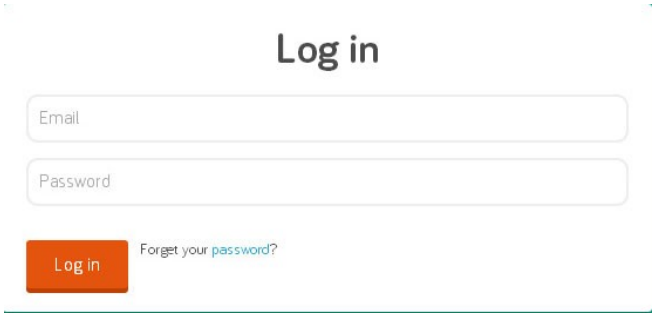
Pada tahap pendaftaran, *pengguna* diwajibkan untuk mempergunakan informasi pribadi yang dimiliki seperti *nama pengguna*, *kata sandi*, PIN 8 digit, alamat e-mail, nomor kartu ID, nomor handphone dan *International Mobile Equipment Identity* (IMEI). Pada beberapa teknik algoritma dilakukan proses pemeriksaan IMEI untuk *handphone* yang digunakan oleh *pengguna*. Jika IMEI palsu, maka *pengguna* akan ditolak untuk melakukan pendaftaran ke dalam sistem. Oleh karena itu, *pengguna* dipaksa untuk dapat memasukkan IMEI asli pada tahap pendaftaran. Kemudian pengguna tidak dapat melakukan pendaftarana jika nomor handphone dan IMEI telah didaftarkan oleh pengguna yang lain. Penggunaan metode ini akan memastikan bahwa setiap *pengguna* memiliki satu nomor *handphone* dan satu nomor IMEI. Sebagian besar sistem authentication memungkinkan pengguna untuk memiliki banyak akun dengan nomor *handphone* yang sama, namun pada sistem yang diusulkan hal tersebut tidak akan terjadi. Kemudian setelah *pengguna* berhasil melakukan pendaftaran, maka *pengguna* akan dibawa pada tahap *login* untuk dapat masuk ke dalam sistem.



Gambar 17. Disain Halaman Pendaftaran

2. Tahap *Login*

Pada tahap *login* pengguna akan masuk ke sistem dengan menggunakan nama pengguna dan kata sandi yang telah dibuat pada tahap pendaftaran, jika pengguna memasukkan kredensial yang salah (nama pengguna atau kata sandi) maka pengguna tidak akan dapat mengakses atau masuk ke dalam sistem. Setelah pengguna memasukkan nama pengguna dan kata sandi yang benar saat tahap pendaftaran, sistem akan mengalihkan secara otomatis ke tahap otentikasi pengguna kedua yaitu tahap konfirmasi.



Gambar 18. Disain Halaman Login

3. Tahap Konfirmasi

Pada tahap ini ini akan mencegah pembuatan OTP oleh server dan mencegahnya untuk dikirim ke pengguna hingga pengguna mengonfirmasi informasi pribadinya seperti PIN, nomor *handphone*, dan IMEI yang telah terdaftar pada tahap pendaftaran. Selain itu, lapisan ini akan memastikan identitas keaslian dan mewujudkan penolakan. Dalam sistem otentikasi lain, setelah pengguna mengirimkan kredensial nama pengguna dan kata sandi ke dalam sistem, maka pengguna akan dapat menerima OTP langsung dari *server* melalui *Short Message Service* (SMS). Sistem yang diusulkan tidak akan menghasilkan OTP dan tidak akan mengirim apapun kepada pengguna sampai sistem memastikan bahwa perangkat *mobile* ada di tangan pengguna yang sama yang meminta otentikasi. Dengan cara ini sistem akan memastikan tanggung jawab orang yang menyalahgunakan sistem. Lapisan ini menggabungkan dua faktor, yaitu *Something you know* berupa PIN dan *Something you have* berupa nomor handphone dan IMEI. Pada tahap ini pengguna dapat memilih metode penerimaan OTP. Jika pengguna memilih untuk tidak menerima OTP melalui SMS, maka dapat menerimanya melalui e-mail. Pengguna akan menerima OTP terenkripsi dengan menggunakan AES 256 dan dekripsi OTP akan dilakukan dengan PIN, yang merupakan kunci simetris antara pengguna dan *server*. Dalam hal pengguna memasukkan informasi yang salah dalam tahap konfirmasi maka akan diarahkan ke login awal dan proses otentikasi akan dimulai kembali.

4. Proses menghasilkan dan pengiriman *one-time password* (OTP)

Kemudian setelah pengguna melewati tahap konfirmasi, server akan menghasilkan OTP dari informasi pengguna. Ini dapat terjadi dalam dua cara. Pengguna dapat memilih untuk menerima OTP melalui *smartphone* atau melalui email. Ini berarti bahwa jika pengguna menggunakan *smartphone* untuk menerima OTP, maka informasi yang diminta dari pengguna pada tahap konfirmasi akan berkontribusi pada pembuatan OTP. *Server* akan mengirim OTP terenkripsi melalui SMS atau e-mail. Setelah pengguna menerima pesan terenkripsi oleh OTP, ia akan mentransfer ke layar lain untuk membuktikan validitas PIN dan pada saat yang sama mendekripsi OTP.

V. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, maka diperoleh kesimpulan bahwa pengembangan user

authentication berbasis *Multi-factor Authentication* (MFA) juga menjadi permasalahan yang dihadapi, setelah dilakukan analisis dan disain dapat disimpulkan bahwa *user authentication* berbasis *Multi-factor Authentication* (MFA) aman dan *user-friendly* yang mampu membedakan pengguna yang diizinkan dan tidak diizinkan untuk menggunakan layanan jaringan *wireless*. Kesimpulan tersebut didapatkan dari hasil analisis yang telah dilakukan dan *user authentication* yang telah dirancangkan sudah memiliki tingkat antisipasi terhadap kejahatan yang cukup baik.

REFERENSI

[1] W. M. G. Kanishka *et al.*, "Wi-Fi Password Two Factor Authentication for Home users (W2FA)," *Int. J. Sci. Res. Publ.*, vol. 6, no. 10, pp. 149–2250, 2016.

[2] M. Rusdan and M. Sabar, "Pengembangan Jaringan Wireless Menggunakan User Authentication Berbasis Radius Dalam Industri 4.0," *Infotech J.*, vol. 5, no. 1, pp. 44–52, 2019.

[3] W. Sudiarto Raharjo, I. D. E.K. Ratri, and H. Susilo, "Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login," *J. Tek. Inform. dan Sist. Inf.*, vol. 3, no. 1, pp. 127–136, 2018.

[4] R. Tulloh, H. Putri, D. A. Nurmantris, and D. D. Prihatin, "SIMULATION Wi-Fi NETWORK WITH WIRELESS DISTRIBUTION SYSTEM (WDS) TOPOLOGY," *Int. J. Comput. Technol.*, vol. 16, no. 5, pp. 6920–6925, 2017.

[5] R. Kumar and N. Tiwari, "An Investigation on Wireless Mobile Network and Wireless LAN (Wi-Fi) for Performance Evaluation," *Int. J. Comput. Appl.*, vol. 126, no. 6, pp. 1–8, 2015.

[6] R. Malhotra, V. Gupta, and R. K. Bansal, "Simulation and Performance Analysis of Wired and Wireless Computer Networks," *Int. J. Comput. Appl.*, vol. 14, no. 7, pp. 11–17, 2011.

[7] W. S. I. Group and P. S. S. Council, "Information Supplement: PCI DSS Wireless Guidelines," *Pci Dss Inf. Suppl.*, no. 2, pp. 1–34, 2011.

[8] O. Bonaventure, *Computer Networking : Principles, Protocols and Practice*. Saylor Foundation, 2011.

[9] P. Sharma, S. Pardeshi, R. Arora, and M. Singh, "A Review of the Development in the Field of Fiber Optic Communication Systems," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 5, pp. 113–119, 2013.

[10] W. Rödiger, T. Mühlbauer, A. Kemper, and T. Neumann, "High-speed query processing over highspeed networks," *Proc. VLDB Endow.*, vol. 9, no. 4, pp. 228–239, 2016.

[11] A. Zappone, M. Di Renzo, and M. Debbah, "Wireless Networks Design in the Era of Deep Learning: Model-Based, AI-Based, or Both?," in *IEEE Transactions on Communications*, 2019, pp. 1–45.

[12] D. Sudipto, *Setting Up of a Wireless Distribution System (WDS)*. 2005.

[13] M. Alizadeh, W. H. Hassan, and T. Khodadadi, "Feasibility of Implementing Multi-factor Authentication Schemes in Mobile Cloud Computing," *Proc. - Int. Conf. Intell. Syst. Model. Simulation, ISMS*, vol. 2015-Septe, pp. 615–618, 2015.

[14] A. Bissada and A. Olmsted, "Mobile Multi-factor Authentication," in *Proceedings 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017*, 2018, pp. 210–211.

[15] T. Mikkonen, S. Andreev, A. Ometov, N. Mäkitalo, Y. Koucheryavy, and S. Bezzateev, "Multi-Factor Authentication: A Survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[16] Sugiyono, *Metode Penelitian Kuantitatif Kualitatif dan R&D*, 10th ed. Bandung: Alfabeta, 2010.

[17] P. S. S. Council, "Multi-factor Authentication," *Encycl. Cryptogr. Secur.*, no. February, pp. 1–10, 2017.

(halaman ini sengaja dikosongkan)