Journal of Applied Informatics and Computing (JAIC)
Vol.5, No.1, Juli 2021, pp. 1~8
e-ISSN: 2548-6861

Pengembangan Layanan Autentikasi Berbasis Teknologi Blockchain

Imam Riadi [1]*, Herman [2], Aulyah Zakilah Ifani [3]****
* Program Studi Sistem Informasi, Universitas Ahmad Dahlan
** Program Studi Teknik Informatika, Universitas Ahmad Dahlan
imam.riadi@is.uad.ac.id [1], hermankaha@mti.uad.ac.id [2], aulyah1908048022@webmail.uad.ac.id [3]

Article Info

Article history:

Received 2020-08-30
Revised 2020-12-17
Accepted 2020-01-27

Keyword:

Autentikasi,
Blockchain,
IEEE 802.1x.

ABSTRACT

The internet is developing so fast, from the kinds of internet technolgy to something that is needed by every user. Information needs and an extensive network system give the easier to access. One of them is wireless, wireless is very helpful for internet users. However, the problem often arises in wireless securing network. Many attacks that make the username and password of the users get hacked. Based on these problems, this study focuses on securing when users login user a device. One of the innovative technologies that be able to solve these problems is Blockchain Technology. By using blockchain technology adversaries will find the difficulty to change and modify the same data on all computers at the same time because it will take the time so long to crack the encryption code on each block of sata on the entire computer network. This study used literature study as a data collection technique. Browsing method using the internet or other network media. This result of this research is the system prototype has been successfully built. The prototype for the development of this login system application has succeed in securing data such as of username and password using blockchain technology. User data is secured and converted into encryption block.

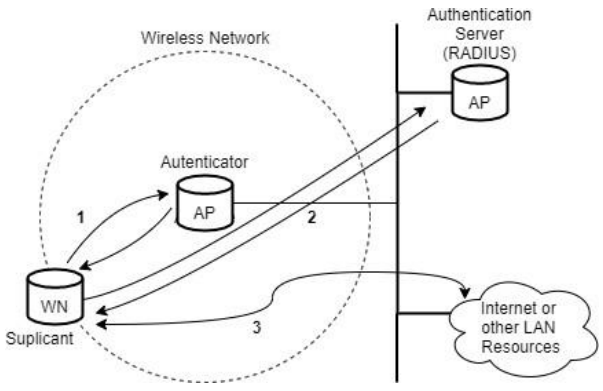
I. PENDAHULUAN

Teknologi akan semakin berkembang terutama internet, banyak pengguna yang menggunakan internet sebagai suatu kebutuhan. Kebutuhan akan informasi dan sistem jaringan yang luas memiliki banyak kemudahan dalam mengaksesnya dan tidak lagi hanya terhubung ke internet melainkan sudah mulai bergeser pada kemampuan mobilitas pengguna yang terhubung dengan internet [1]. Untuk melayani pengguna yang mobile dibutuhkan jaringan *wireless*. Jaringan *wireless* dapat diakses menggunakan smartphone, laptop, dan peralatan mobile lainnya [2]. Kelebihan jaringan *wireless* dalam hal mobilitas penggunanya juga dihadapkan pada beberapa tantangan. Salah satu tantangan besarnya adalah dalam hal pengamanan jaringan *wireless* tersebut, dimana banyak sekali serangan secara ilegal untuk mendapatkan *username* dan *password* dari pengguna [2]. Salah satu teknologi inovasi yang mampu menyelesaikan permasalahan tersebut adalah Teknologi *Blockchain*. Teknologi *blockchain* membuat peretas akan sulit mengubah dan memodifikasi data yang sama disemua komputer di saat yang sama karena membutuhkan waktu yang sangat lama untuk memecahkan kode enkripsi pada setiap blok data di seluruh jaringan komputer.

Dibalik teknologi *blockchain* terdapat 6 karakteristik utama. Pertama, *blockchain* menerapkan kriptografi untuk memastikan keamanan setiap transaks. *Blockchain* adalah akuntansi yang mencatat transaksi-transaksi keuangan (*monetary)* dan data penting lainnya. Kemudian, *Blockchain* adalah rantai, dimana *blockchain* terdiri dari kumpulan blok, setiap blok yang baru tersambung ke blok yang sebelumnya membentuk struktur rantai. Data transaksi dalam *Blockchain* tersimpan pada sebuah buku besar yang terdistribusi ke seluruh nodes dan sulit dimanipulasi oleh *adversaries*. *Blockchain* adalah *mining* karna setiap pihak yang berhasil melakukan validasi kebenaran transaksi dan mencantumkannya pada blok baru, akan mendapatkan imbalan *crypto coin*. Terakhir, *Blockchain* adalah *smart contract* karena selain menyimpan data dan transaksi, *blockchain* juga bisa mengeksekusi kontrak perjanjian yang telah disimpan sebelumnya [3].

Teknologi *blockchain* telah diterapkan pada banyak bidang kehidupan. Pada bidang sosial, *blockchain* digunakan untuk *platform crowfunding*. Banyak kampanye program sosial yang disertai penggalangan dana telah menggunakan *platform* ini. Penggunaan teknologi ini untuk mendigitalkan hak properti dan aset fisik menggunakan *jaringan peer-to-peer* sehingga dapat melindungi dana dari investor. Jaringan *peer-to-peer* melakukan transaksi terdesentralisasi pada layanan keuangan pada pembuat project [4]. Berbagai aplikasi teknologi *blockchain* sangat berkembang dalam bidang kesehatan, *Internet of Things* (IoT), pengolaan aset digital, dll [5]. *Blockchain* juga digunakan dalam meningkatkan keamanan sistem *e-commerce* [6] dan juga sistem *e-voting* [7]. *Blockchain* menjadi opsi dalam perdagangan elektronik yang terjadi antara konsumen. *Blockchain* dapat memberikan kepercayaan terhadap pihak ketiga yang mengawasi proses antara penjual dan pembeli untuk mengkonfirmasi keaslian data dan informasi [8]. Keunggulan dari aplikasi teknologi *blockchain* adalah sifat yang *public* artinya setiap orang bisa menjadi validator dalam pelaksanaan konsensus protokol, *decentralized* artinya data transaksi dalam *blockchain* tidak disimpan di satu penyimpanan data terpusat, melainkan tersebar di setiap *full node blockchain*. *Immutable* artinya setiap transaksi yang sudah tercatat dalam *blockchain* tidak dapat diubah lagi. Smart *contract* yang mampu memfasilitasi, memverifikasi dan meng-eksekusi kontrak antara pihak-pihak yang berkomitmen [9].

Dalam kaitannya dengan implementasi *blockchain*, jaringan *wireless* saat ini menerapkan protokol IEEE 802.1x. protokol tersebut menggunakan *server* autentikasi untuk mengautentikasi koneksi antara *access point* dan *station*. Komunikasi *access point* dan autentikasi *server* diimplementasikan menggunakan protokol berbeda [10]. Protokol IEEE 802.1x memiliki 2 *entitas port* logis yaitu *port* terkontrol yang merupakan tempat 802.1x untuk mengizinkan ataupun menolak lalu lintas data yang mengalir berdasarkan status otentikasi *port*. Kedua, *port* yang tidak terkontrol digunakan untuk mengirim *Frame Eapol* (kontrol lalu lintas) dimana frame eapol digunakan dalam pertukaran pengirim dan pengautentikasi [11].



Gambar 1. Skema Arsitektur IEEE 802.1x

Gambar 1 menggambarkan proses autentikasi koneksi IEEE 802.1x yang menggunakan *protocol Remote Authentication Dial-in User Service* (RADIUS). Prosedur autentikasi melibatkan tiga komponen dalam melakukan prosedur otentikasi yaitu *supplicant, authenticator, authenticator server* (RADIUS).

Skema arsitektur 802.1x menunjukkan *supplicant* yang merupakan perangkat laptop dan yang lainnya yang biasanya digunakan pengguna untuk menyambungkan diri ke perangkat *authenticator* berupa *access point.* Dari koneksi *supplicant* dan *authenticator* akan ada menu untuk memasukkan *username* dan *password* untuk koneksi ke jaringan. Kemudian *authenticator* akan meneruskan data baru *user* itu ke *authentication server* yang berupa RADIUS *server*. RADIUS *server* digunakan untuk menyimpan *username dan password* secara terpusat yang akan melakukan autentikasi *client* yang akan melakukan *login* ke jaringan. RADIUS *server* yang menentukan dapat tidaknya pengguna terkoneksi jaringan [12].

Blockchain memungkinkan transaksi antara A dan B terjadi tanpa perantara, lebih aman dan dengan biaya yang lebih murah [13]. *Blockhain* merupakan *tamper-proof block* yang disimpan pada setiap simpul (nodes) yang berpartisipasi dalam jaringan *peer-to-peer blockchain* tersebut. Setiap blok dari *blockchain* merekam ratusan transaksi beserta dengan metadata yang berkaitan [14]. Blok demi blok yang berisi transaksi data ini selanjutnya membentuk rantai blok yang berisi (*blockchain)* [15]. Dalam pembentukan rantai blok ini, setiap blok baru terikat ke blok sebelumnya. Ikatan ini sibuat dengan menyimpan *hash* dari blok sebelumnya pada *header* blok yang baru. Blok pertama dari sebuah *blockchain* disebut blok *genesis.* Karena yang pertama, blok *genesis* merupakan satu-satunya blok tidak menyimpan *hash* dari blok sebelumnya [16]. *Blockchain* menerapkan algoritma kriptografi untuk menjaga keamanan untaian blok-blok dalam *blockchain.* algoritma ini juga memungkinkan sistem melacak seandainya terjadi sabotase terhadap rantai blok [17].

Setiap transaksi dalam *blockchain* akan melewati tiga fase. Pertama klien membuat sebuah transaksi. Transaksi akan disebarluaskan ke simpul-simpul *(nodes)* yang lain secara *peer-to-peer.* kedua, salah satu simpul yang sukses menjalankan konsensus protokol (*miner)* akan memastikan transaksi itu masuk dalam blok baru yang dia cantumkan pada rantai *blockchain.* Ketiga, blok yang baru dibuat tersebut dikirim ke setiap node yang selanjutnya akan ditambahkan oleh setiap node itu ke rantai *local blockchain.* Dengan kata lain transaksi yang ada dalam blok baru akan ditambahkan oleh node ke buku besar mereka masing-masing [14]. Keuntungan dari *blockchain* terdapat pada layanan pemantauan dan keamanan autentikasi, kerahasiaan privasi integritas. Teknologi *blockchain* ini memberikan jaminan keamanan dengan menyediakan solusi yang sepenuhnya terdistribusi, terbukti aman dan konsensus. [18]. Teknologi *blockchain* jika dibandingkan dengan teknologi konvensional lebih unggul ketika diaplikasikan pada berbagai jenis sektor industri, contohnya jasa keuangan dan juga *supply chain* [17].

Authentication adalah pembuktian terhadap identitas suatu entitas contohnya kartu kredit atau mesin, dan orang [2]. Berikut konsep autentikasi:

Gambar 2. Konsep Authentication [2]

Gambar 2 menunjukkan contoh autentikasi pengguna dimana ada *ownership* atau sesuatu yang dimiliki oleh pengguna contohnya *access card with photo. Knowledge* atau sesuatu yang dimiliki oleh pengguna contohnya *username* dan *password*. *Biometric* atau sesuatu yang ada pada pengguna contohnya sidik jari, DNA atau aspek lain yang *menyangkut biometric* [2]. Autentikasi dibagi menjadi tiga kategori diantaranya yaitu: pertama, *What the entity knows* contoh berupa kata sandi, kedua *What the entity owns* seperti kartu pintar, kunci privasi atau tiket karberos, dan ketiga *What the entity* yang mencakup teknik otentikasi berdasarkan fitur *biometric* pengguna (sidik jari, bentuk wajah, bentuk tangan, dll) [19].

Penelitian ini menggunakan literature review sebagai teknik pengumpulan data. Metode penelusurannya menggunakan internet atau *media* jaringan lainnya. Berdasarkan uraian diatas tujuan dari penelitian ini untuk mengembangkan sebuah aplikasi *login* dengan menggunakan Teknologi *Blockchain.*

II. METODOLOGI PENELITIAN

A. Subjek Penelitian

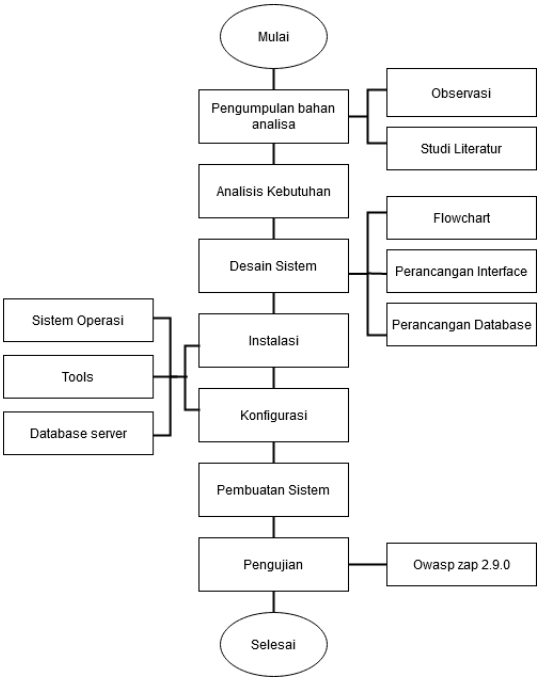
Subjek yang akan dibahas pada penelitian ini adalah prototype pengembangan autentikasi *login* dengan menggunakan teknologi *blockchain*. Dengan menggunakan teknologi *blockchain* diharapkan dapat digunakan sebagai pengamanan sistem *login* pada *wireless*.

B. Analisis Kebutuhan Sistem

Analisis kebutuhan sistem teridiri dari perangkat keras dan perangkat lunak. Perangkat keras meliputi laptop sebagai *station* atau pengguna sedangkan perangkat lunak meliputi windows 10 pro sebagai sistem operasi, php sebagai aplikasi bahasa pemrograman, MySQL sebagai aplikasi *database*, Xampp.

C. Tahapan Penelitian

Tahapan penelitian sebagai alur proses layanan ieee 802.1x berbasis teknologi *blockchain* dapat dilihat pada gambar 3.



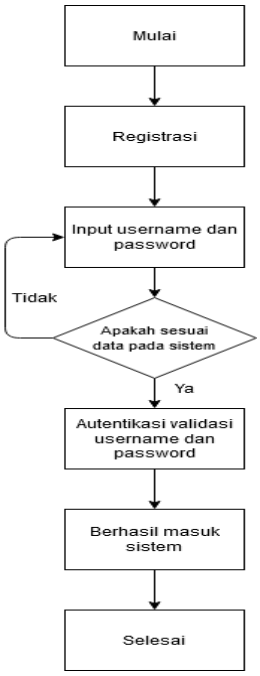
Gambar 3. Alur proses layanan autentikasi berbasis blockchain

Alur proses layanan autentikasi berbasis blockchain yang pertama dilakukan yaitu pengumpulan bahan analisis, tahapan ini melakukan analisis dengan menggunakan observasi dan studi literatur. Studi literatur bisa didapatkan dari berbagai jurnal, buku, prosiding, internet, dll. Analisa kebutuhan menggambarkan kebutuhan apa saja yang dibutuhkan oleh sistem. Tahapan desain sistem menghasilkan desain flowchart, perancangan interface, dan juga perancangan database. Tahapan instalasi dilakukan agar dapat membuat sistem sesuai dengan yang dibutuhkan dan tahapan konfigurasi dilakukan untuk mempersiapkan sistem operasi, tools dan database server yang akan digunakan untuk melakukan pengembangan sistem. Setelah itu menuju pembuatan login. Pembuatan sistem diimplementasikan dengan menggunakan bahasa pemrograman php. Selanjutnya tahapan terakhir adalah tahapan pengujian yang menggunakan OWASP zap 2.9.0.

D. Desain Flowchart

Desain flowchart sistem menggambarkan alur kerja sistem yang akan dirancang. Sistem mempunyai kemampuan untuk melakukan pengecekan data yang ada pada sistem blockchain. Berikut perancangan flowchart sistem dapat di lihat pada gambar 4.

Gambar 4 merupakan tahapan flowchart sistem, pertama pengguna atau user akan melakukan login terlebih dahulu. Setelah login pengguna menginputkan username dan password.

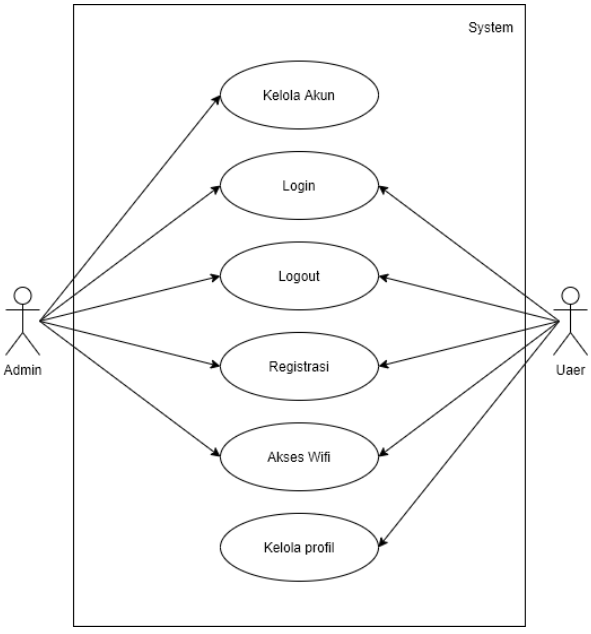


Gambar 4. Flowchart Sistem

Sistem akan mengecek apakah data yang ada pada sistem blockchain jika data yang dimasukkan sudah benar maka sistem akan melakukan autentikasi validasi username dan password setelah semua proses selesai maka pengguna akan mendapatkan koneksi internet.

E. Use case Diagram

Use case digunakan untuk menjelaskan hubungan antara pengguna atau aktor yang terlibat dengan sistem yang akan dibuat.

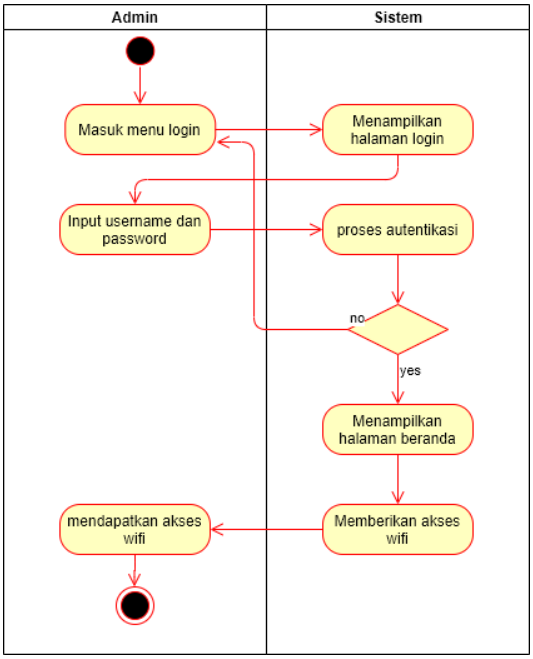


Gambar 5. Use Case Diagram

Pada penelitian ini menampilkan admin dan user, dimana terdiri dari kelola akun, login, logout, registrasi, akses wifi, lihat profil. Use case diagram penelitian ini dapat dilihat pada gambar 5.

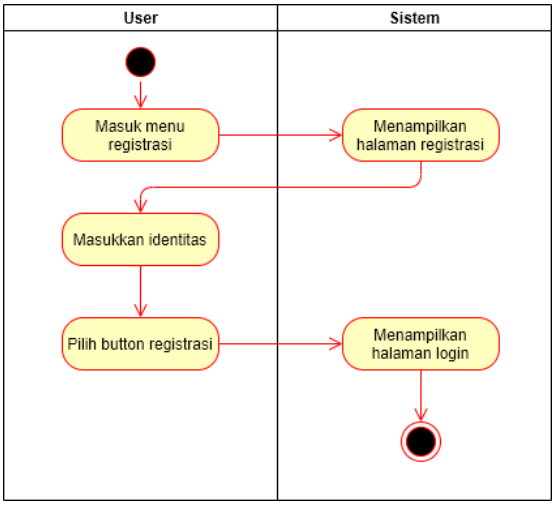
F. Activity Diagram

Activity diagram bertujuan untuk menggambarkan aktivitas yang terjadi pada sistem. Activity diagram terdiri dari tahapan menjalankan sistem setiap interface dibuat untuk mempermudah user menggunakan sistem.



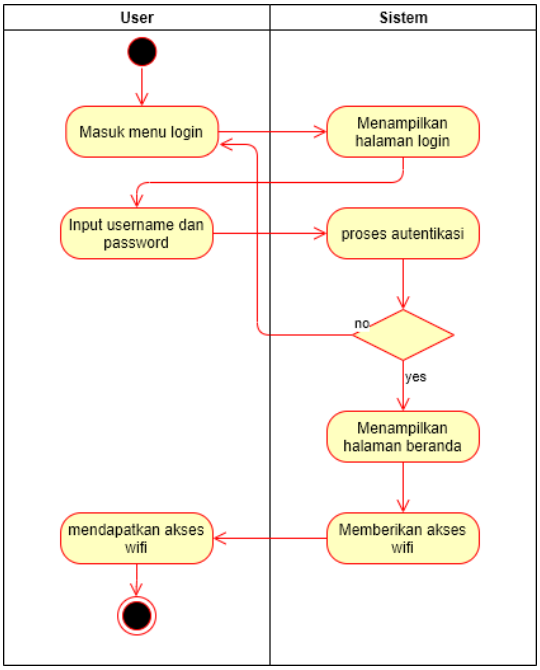
Gambar 6. Activity diagram form login admin

Gambar 6 merupakan proses login dimulai dari admin masuk ke menu login lalu mengisi form login yang berisi inputan username dan password. Setelah itu, data username dan password diterima oleh sistem lalu dilakukan proses pengecekan atau autentikasi, jika valid maka akan melanjutkan ke halaman beranda jika tidak valid maka admin tidak bisa melanjutkan masuk ke sistem. Setelah datanya valid maka akan mendapatkan akses wifi.



Gambar 7. Activity diagram form registrasi

Gambar 7 merupakan proses untuk melakukan registrasi bagi pengguna baru atau yang belum memiliki akun. Proses tersebut dimulai dari masuk menu registrasi lalu mengisi identitas berupa first name, last name, username, password, dan tanggal lahir. Setelah mengisi identitas lalu user mengklik button registrasi dan selanjutnya sistem akan menampilkan halaman login.



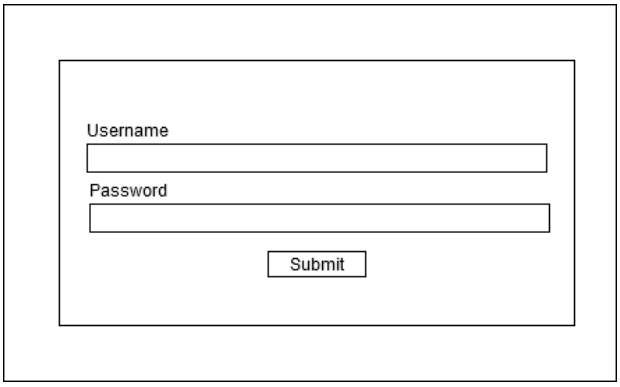
Gambar 8. Activity diagram form login user

Gambar 8 menunjukan user ketika memiliki akun, selanjutnya akan ditampilkan halaman login. Pertama user akan menginputkan username dan password lalu akan dilakukan pengecekan atau autentikasi oleh sistem setelah datanya valid user akan diarahkan ke halaman beranda dan mendapatkan akses wifi.

G. Desain User Interface

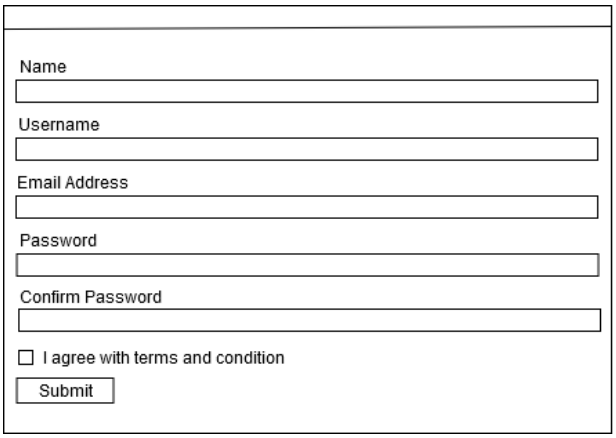
Desain user interface menjelaskan mengenai antar muka dari sistem yang nantinya akan dibuat sebelum diimplementasikan dengan menggunakan bahasa pemrograman php. Rancangan antar muka ini terdiri dari beberapa bagian penting dalam sistem, pada bagian ini akan digambarkan mengenai tampilan yang akan di implementasikan. Sistem yang digunakan dalam pembuatan rancangan ini dengan menggunakan aplikasi figma. Kelebihan Figma yaitu mudah digunakan, fitur-fitur yang ada tidak harus di download, dan penggunaanya yang gratis. Perancangan komponen sistem yang akan digambarkan dalam bagian ini meliputi form login, halaman registrasi, halaman awal, lihat profil. Sedangkan untuk implementasi sistem menggunakan bahasa pemrograman php. Pengujian sistem menggunakan tool OWASP.

Halaman awal dari sistem yang dibangun merupakan langkah pertama yang akan ditampilkan sebelum masuk ke halaman login berhasil. Halaman ini berisikan username, password, login, dan juga terdapat menu registrasi. Halaman awal ini digunakan ketika user atau admin akan memasukkan username dan password untuk mendapatkan koneksi internet dan bisa masuk ke dalam sistem. Apabila user telah memasukkan username dan password dengan benar maka langkah selanjutnya menekan tombol submit agar dapat dialihkan ke halaman login berhasil. Apabila user belum memiliki username dan password, maka terlebih dahulu melakukan registrasi dengan menekan tombol registrasi. Menu registrasi digunakan untuk mendaftarkan username dan password dari pengguna agar pengguna dapat login menggunakan sistem. Untuk halaman awal dapat dilihat pada gambar 9 sedangkan untuk halaman registrasi dapat dilihat pada gambar 10.



Gambar 9. Halaman awal login

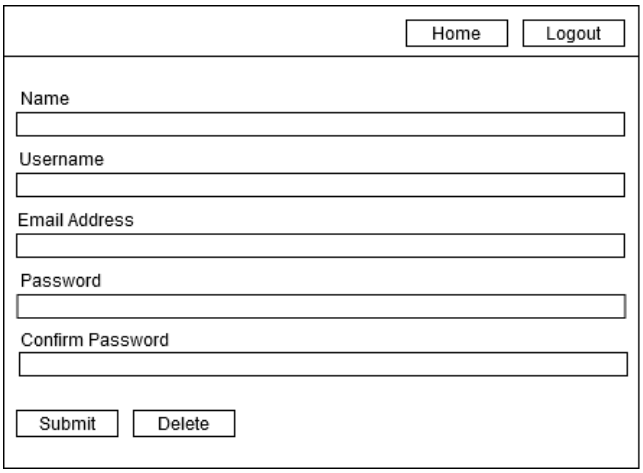
Halaman awal login digunakan untuk pengisian username dan password harus sesuai dengan data yang ada di dalam database server. Sehingga dibutuhkan menu untuk melakukan registrasi. Halaman registrasi dibuat sesuai dengan yang dirancang sebelumnya menggunakan figma. Halaman registrasi digunakan untuk mendaftarkan username dan password sebelum masuk kedalam sistem. Dalam halaman registrasi terdapat name, username, email address, password, confirm password, dan submit. Berikut gambar 10 halaman registrasi.



Gambar 10. Halaman Registrasi

Gambar 10 digunakan ketika user belum memiliki akun untuk mengakses sistem. Setelah mengisi biodata selanjutnya user menekan tombol registrasi maka akan diarahkan ke halaman awal atau halaman beranda. Halaman awal terdiri

dari biodata yang telah diisikan sebelumnya. Pengguna juga dapat mengganti biodata. Dapat dilihat pada Gambar 11

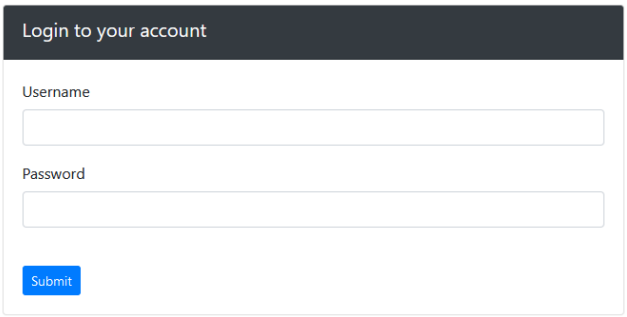


Gambar 11. Halaman login berhasil

Halaman login berhasil berisikan biodata dari pengguna. Pengguna dapat mengubah nama dan password dan selanjutnya akan disimpan ke dalam database. Setelah melakukan perancangan sistem, selanjutnya akan dilakukan implementasi sistem dengan menggunakan php. Sistem yang dibangun akan dilakukan uji vulnerability dengan menggunakan tool OWASP.

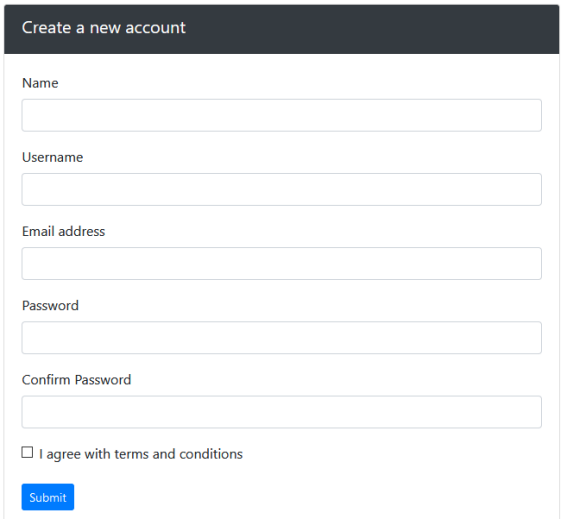
III. HASIL DAN PEMBAHASAN

Bagian ini merupakan tampilan dari aplikasi yang sudah dibuat menggunakan bahasa pemrograman php. Hasil tahapan implementasi merupakan sebuah sistem yang siap diuji dan dijalankan. Halaman awal dari sistem yang dibangun merupakan langkah pertama yang akan ditampilkan sebelum masuk ke halaman login berhasil. Halaman ini dibuat untuk memberikan batasan kepada pihak yang tidak berkepentingan agar tidak dapat mengakses dan mengolah data tanpa melakukan login terlebih dahulu. Sehingga sebelum melakukan login pengguna melakukan registrasi terlebih dahulu untuk mendapatkan akun. Gambar 12 merupakan tampilan menu login.



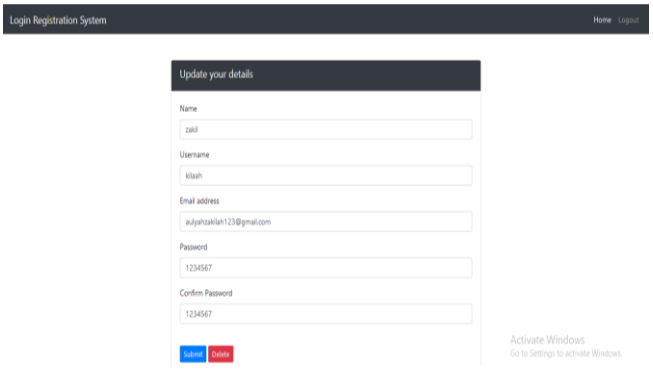
Gambar 12. Halaman awal

Halaman registrasi digunakan untuk mendaftarkan username dan password sebelum masuk ke sistem. Halaman registrasi merupakan gambaran awal ketika pengguna belum memiliki akun login. Halaman registrasi teridir dari beberapa yang harus di isikan. Berikut gambar 13 halaman registrasi.



Gambar 13. Desain Halaman Registrasi

Gambar 13 terdiri dari name, username, email address, password dan confirm password. Setelah melakukan registrasi maka user akan diarahkan ke halaman awal atau halaman beranda.

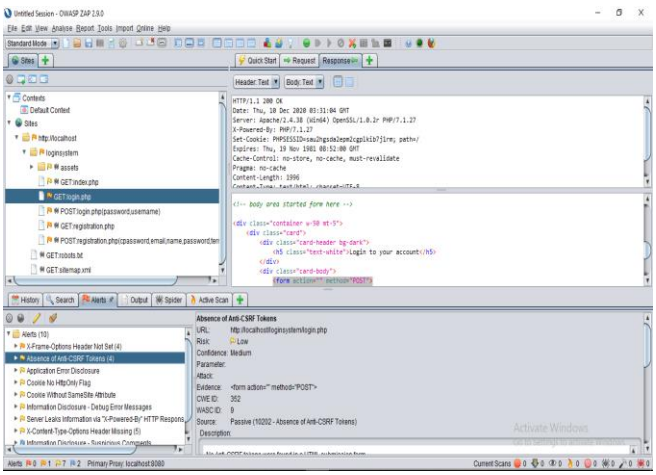


Gambar 14. Login Berhasil

Halaman login berhasil digunakan untuk melihat biodata user. Ketika user berhasil maka menandakan user berhasil masuk kedalam sistem. Tombol delete digunakan ketika user telah mengubah data profile. Sedangkan tombol submit untuk menyimpan data yang sudah diubah. Terdapat tombol home dan logout. Tombol logout digunakan ketika selesai menggunakan sistem. Tombol home ketika ingin kembali ke halaman login.

Pengujian sistem menggunakan tool OWASP ZAP yang bertujuan mencari celah kerentanan atau vulnerability pada website, server, dan lain-lain. Bagian alert pada gambar diatas menampilkan 3 bagian celah kerentanan atau vulnerability, diantaranya high risk, medium risk, low risk. Menghasilkan alert di antaranya: Cross Domain Misconfiguration, X-Frame-Options Header Not Set, Absence of Anti CSRF Token, Cookie No Http Only Flag, Cookie Without SameSite Attribute, Cookie Without Secure Flag, Incomplete or No

Cache-control & Pragma HTTP Header Set, Information Disclusure-Debug Error Message, Server Leaks Information via X-Powered By HTTP Respons Header Field(s), X-Content-Type-Options Header Message. Seperti ditampilkan pada gambar 15.



Gambar 15. Hasil scanning oleh OWASP, diperoleh 10 (sepuluh) sub file sistem yang terindikasi memiliki vulnerability

Hasil analisis atau Result Analysis yang didapatkan dari pengujian menggunakan OWASP mendeteksi 10 subfile vulnerability, high, medium, low. Tabel 1 merupakan pengujian yang telah dilalukan pada sistem yang telah dibuat.

TABEL I
PENGUJIAN DENGAN OWASP

No	Nama Subfile SistemVulnerability	Risk		
		High	Medium	Low
1	Cross Domain Misconfiguration		15	
2	X-Frame-Options Header Not Set		4	
3	Absence of Anti CSRF Token			4
4	Cookie No Http Only Flag			1
5	Cookie Without SameSite Attribute			70
6	Cookie Without Secure Flag			106
7	Incomplete or No Cache-control & Pragma HTTP Header Set			19
8	Information Disclusure-Debug Error Message			1
9	Server Leaks Information via X-Powered by HTTP Respons Header Field(s)			6
10	X-Content-Type-Options Header Message		49	

Hasil *scanning* mendeteksi 10 *vulnerability* secara keseluruhan pada Sistem Login, menggunakan tool OWASP. Rekomendasi atau *countermeasure* untuk perbaikan sistem login. Countermeasure merupakan saran atau rekomendasi yang diberikan oleh *tool* OWASP yang memiliki standar kualitas tinggi pada bidang *IT Security* [20].

TABEL II
PENGUJIAN DENGAN OWASP

No	Nama Subfile Sistem Vulnerability	Jumlah Vulnerability	Rekomendasi perbaikan (*Countermeasure)*
1	Cross Domain Misconfiguration	15	Refrensi OWASP
2	X-Frame-Options Header Not Set	4	Pastikan filter XSS *browser Web* diaktifkan dengan mengatur header respons X-XSS-Protection HTTP ke 1
3	Absence of Anti CSRF Token	4	Refrensi OWASP
4	Cookie No Http Only Flag	1	Pastikan bahwa sistem menyetel header Content-tyPe secara tepat dan itu menetapkan header X-Content-Type-Options ke ‘nosniff’ untuk semua halaman web. Jika memungkinkan, pastikan bahwa pengguna akhir menggunakan browser web standar-compliant.
5	Cookie Without SameSite Attribute	70	Referensi OWASP
6	Cookie Without Secure Flag	106	Referensi OWASP
7	Incomplete or No Cache-control & Pragma HTTP Header Set	19	Referensi OWASP
8	Information Disclusure-Debug Error Message	1	Refrensi OWASP
9	Server Leaks Information via X-Powered By HTTP Respons Header Field(s)	6	Refrensi OWASP
10	X-Content-Type-Options Header Message	49	Refrensi OWASP
Total	275		

V. KESIMPULAN

Penelitian mengenai aplikasi sistem login ini menggunakan aplikasi *figma* untuk membuat desainnya dan implementasi sistem menggunakan *PHP*. Rancangan prototype telah berhasil dibangun. Prototype ini bisa dijadikan sebagai metode alternatif dalam melakukan proses login, dimana data dari pengguna dapat diamankan dengan teknologi blockchain yang mengubah data tersebut menjadi blok enkripsi. Sistem ini juga dilengkapi dengan menu lihat profil yang didalamnya dapat digunakan untuk mengubah *username* dan *password* dari pengguna. Sistem ini dilengkapi dengan menu registrasi yang digunakan untuk pendaftaran user atau pengguna. Ketika *username* dan *password* tersimpan dalam database dan pengguna melakukan login maka pengguna akan berhasil login. Ketika data yang dimasukkan salah maka proses login akan gagal. Pengujian menggunakan *tool OWASP zap* yang memiliki 3 tingkat kerentanan, yaitu *high*, *medium*, *low*. Tingkat kerentanan diperoleh dari notifikasi alert yang ditampilkan oleh *tool* OWASP. Hasil pengujian pada sistem login diperoleh *tool* OWASP kerentanan *high* 0, kerentanna medium 68, kerentanan *low* 256. Total celah katau *vulnerability* yang ditemukan berjumlah 275. Hasil pengujian yang dilakukan menunjukkan bahwa pada sistem login yang telah dibangun dapat direkomendasikan untuk digunakan.

DAFTAR PUSTAKA

[1] Y. N. Kunang dan T. Ibadi, "Celah Keamanan Sistem Autentikasi Wireless Berbasis RADIUS," Celah Keamanan Sist. Autentikasi Wirel. Berbas. Radius, vol. 34, no. 2, hal. 1907–5022, 2013.

[2] M. Rusdan dan M. Sabar, "Analisis dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication," Jt. (Journal Inf. Technol., vol. 02, no. 01, hal. 17–24, 2020.

[3] U. Rahardja, E. P. Harahap, dan D. D. Christianto, "Pengaruh Teknologi Blockchain Terhadap Tingkat Keaslian Ijazah," Technomedia J., vol. 4, no. 2, hal. 211–222, 2019.

[4] E. P. Harahap, Q. Aini, dan R. K. Anam, "Pemanfaatan Teknologi Blockchain Pada Platform Crowdfunding," Technomedia J., vol. 4, no. 2, hal. 199–210, 2019.

[5] L. Ismanto, H. S. Ar, A. N. Fajar, Sfenrianto, dan S. Bachtiar, "Blockchain as E-Commerce Platform in Indonesia," J. Phys. Conf. Ser., vol. 1179, no. 1, 2019.

[6] X. Zhu dan D. Wang, "Research on Blockchain Application for E-Commerce, Finance and Energy," IOP Conf. Ser. Earth Environ. Sci., vol. 252, no. 4, 2019.

[7] A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam, dan A. Islam, "Towards Blockchain-Based E-voting System," 2018 Int. Conf. Innov. Sci. Eng. Technol. ICISET 2018, hal. 351–354, 2018.

[8] S. Shorman, M. Allaymoun, dan O. Hamid, "Developing the E-Commerce Model a Consumer To Consumer Using Blockchain Network Technique," Int. J. Manag. Inf. Technol., vol. 11, no. 02, hal. 55–64, 2019.

[9] Y. W. Chang, K. P. Lin, dan C. Y. Shen, "Blockchain Technology for e-Marketplace," 2019 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2019, hal. 429–430, 2019.

[10] M. A. Abdillah, A. Yudhana, dan A. Fadil, "Sniffing Pada Jaringan WiFi Berbasis Protokol 802.1x Menggunakan Aplikasi Wireshark," J-SAKTI (Jurnal Sains Komput. dan Inform., vol. 4, no. 1, hal. 1, 2020.

[11] R. Sundaramoorthy, K. Rajapandiyan, V. Palanivelayudham, dan U. Muthukrishnan, "Interoperability Solution for Ieee 802.1x Based Authentication Unsupported Customer Premises Equipment," Proc. 2019 3rd IEEE Int. Conf. Electr. Comput. Commun. Technol. ICECCT 2019, hal. 1–5, 2019.

[12] I. Wiratama dan P. Sugiartawan, "Peningkatan Keamanan Wireless Pada Jaringan Komputer di Universitas Amikom Menggunakan Protokol IEEE802.1X," J. Sist. Inf. dan Komput. Terap. Indones., vol. 2, no. 1, hal. 155–164, 2019.

[13] U. Rahardja, Q. Aini, M. Yusup, dan A. Edliyanti, "Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce," Comput. Eng. Sci. Syst. J., vol. 5, no. 1, hal. 28–32, 2020.

[14] S. Gupta dan M. Sadoghi, "Encyclopedia of Big Data Technologies," Encycl. Big Data Technol., no. May, 2020.

[15] S. Damai dkk., "Implementasi Blockchain : Studi Kasus e-Voting," J. Infra Petra, no. 031, 2019.

[16] O. Novo, "Scalable access management in IoT using blockchain: A performance evaluation," IEEE Internet Things J., vol. 6, no. 3, hal. 4694–4701, 2019.

[17] N. I. Fauzan, "Teknologi Blockchain Dan Peranannya Dalam Era Digital," vol. 4, hal. 1–15, 2018.

[18] T. Salman, M. Zolanvari, A. Erbad, R. Jain, dan M. Samaka, "Security services using blockchains: A state of the art survey," IEEE Commun. Surv. Tutorials, vol. 21, no. 1, hal. 858–880, 2019.

[19] W. S. Raharjo, I. D. E. K. Ratri, H. Susilo, J. Wahidin, dan S. Yogyakarta, "Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login," vol. 3, no. April, hal. 127–136, 2017.

[20] H. Han, C. Wu, S. Gao, dan G. Zu, "An assessment approach of the power system vulnerability considering the uncertainties of wind power integration," China Int. Conf. Electr. Distrib. CICED, no. 201804270000656, hal. 741–745, 2018.