Desain Konseptual Sistem Pembatasan Akses Laboratorium Berbasis Teknologi Biometrik dan Monitoringnya Secara Jarak Jauh Berbasis IoT untuk Mendukung Kondisi *Work From Home (WFH)*

Rina Mardiati[1], Nanang Ismail[2], Adam Faroqi[3], Mufid Ridlo Effendi[4]

[1,2,3,4]Jurusan Teknik Elektro, UIN Sunan Gunung Djati Bandung, Indonesia

e-mail: [1]r_mardiati@uinsgd.ac.id, [2]nanang.is@uinsgd.ac.id, [3]adam.faroqi@uinsgd.ac.id, [4]mufid.ridlo@uinsgd.ac.id

Abstrak

Sistem keamanan laboratorium pada umumnya menggunakan kunci konvensional, alarm, dan CCTV. Sistem keamanan laboratorium yang konvensional tidak dapat membatasi pengguna laboratorium dan memantau siapa saja yang menggunakan laboratorium. Makalah ini mengusulkan sebuah desain konseptual sistem pembatasan akses laboratorium berbasis teknologi biometrik dan sistem monitoringnya secara jarak jauh berbasis IoT. Monitoring jarak jauh terhadap siapa saja yang mengakses laboratorium menjadi hal yang sangat penting untuk membantu kondisi pengawasan dan pengamanan laboratorium pada kondisi *Work From Home (WFH)*. Pengelola laboratorium dapat mengetahui siapa saja yang masuk dan jam berapa melakukan aktivitas di lab dari rumah. Jika ada yang memaksa melakukan akses paksa terhadap laboratorium akan segera dapat dimonitor oleh pengelola.

Kata kunci: keamanan, laboratorium, biometrik, monitoring, IoT

1 Pendahuluan

Laboratorium merupakan salah satu tempat dilakukannya pengembangan-pengembangan ilmu pengetahuan dengan perangkat-perangkat spesifik dengan harga yang tidak murah. Pengamanan laboratorium sangat diperlukan untuk mengamankan perangkat-perangkat di dalamnya dan masuknya orang-orang yang tidak berkepentingan. Apalagi dalam kondisi sedang ada wabah, dimana mayoritas kantor dan institusi pendidikan ditutup dan beralih pada skema *Work From Home (WFH)* dan pembelajaran jarak jauh. Maka pembatasan dan pengamanan akses ke laboratorium harus lebih diperketat, hanya orang-orang tertentu yang dibolehkan mengakses laboratorium dalam jumlah dan waktu yang terbatas.

Sistem keamanan laboratorium yang banyak digunakan saat ini yaitu menggunakan *Closed Circuit Television* (CCTV) dengan tujuan merekam semua kejadian di sekitar laboratorium dengan jangkauan pengamatan terbatas. Selain itu, CCTV hanya dapat merekam kejadian tanpa dapat memberikan peringatan kepada penjaga laboratorium jika terjadi hal-hal yang membahayakan. Sehingga, penelitian mengenai pengembangan sistem keamanan dengan CCTV sebagai alat untuk *data ghatering* pun mulai dikembangkan. Misalnya penelitian yang dilakukan oleh Khresna dkk. yang mengkombinasikan CCTV dengan teknologi SMS *gateway* untuk keamanan rumah (Kresnha, Susilowati, & Mujiastuti, 2018). Pemanfaatan CCTV juga bisa dihubungkan dengan *cloud system* untuk penyimpanan dan pengolahan datanya (Asror & Siradj, 2016). Selain dapat dikombinasikan dengan teknologi SMS Gateway dan *cloud system*, CCTV juga bisa dikombinasikan dengan berbagai teknologi lainnya untuk pengawasan, seperti penggunaan sensor PIR (Syahidulhaq, Hafiddudin, & Aulia, 2016), teknologi seluler dan *smartphone* (Dewa & Kartadie, 2016), dan lainnya.

CCTV digunakan untuk memantau pergerakan berbasis video, tetapi teknologi ini tidak bisa digunakan secara langsung untuk pembatasan akses masuk suatu area atau ruangan. Kalaupun bisa, maka ia harus dikombinasikan dengan teknologi deteksi wajah yang tentu tidak sederhana jika objeknya dinamis, banyak melakukan pergerakan. Teknologi untuk membatasi akses terhadap laboratorium yang dapat digunakan adalah teknologi biometrik, baik biometrik fisik seperi retina, sidik jari, wajah, dan DNA, mapun biometrik perilaku seperti suara, gesture, dan cara mengetik (Hill, 2015), (Siswanto, Efendi, & Yulianti, 2018).

Dalam hal komunikasi dan pengolahan data, saat ini sudah banyak pilihan teknologi yang bisa digunakan, seperti SMS Gateway, IoT (Pasha, et al., 2018) (Gunawan, et al., 2017), Cloud system, Wifi (Haryanto, Ismail, & Pristianto, 2018), dan teknologi seluler (Kamelia, S.R, W.S, & Mulyana, 2014). Beberapa penelitian sudah mencoba melakukan kombinasi tersebut. Dony Saputra, dkk. membuat suatu sistem keamanan ruangan menggunakan sidik jari dan sensor gerak dengan kontroler mikrokontroler (Saputra, Masud, Ramdhan, & Fitriani, 2014). Usman, dkk merancang pagar otomatis dengan sensor sidik jari menggunakan mikrokontroler yang akan memicu motor penggerak pagar (Usman, Rahmansyah, & Apriadi, 2017). Sementara itu, Tobing, dkk dalam papernya (Tobing, 2014), merancang pengamanan pintu menggunakan sidik jari yang hanya dapat diakses oleh anggota keluarga. Selain itu sistem keamanan ini juga dapat dikendalikan melalui smartphone android yang telah diinstal aplikasi dengan menggunakan modul bluetooth. Pemanfaatan sidik jari juga dilakukan oleh Cahyono, dkk dalam penelitiannya yang membuat sistem keamanan brankas yang diatur oleh mikrokontroler (FA & P, 2016). Alat ini menggunakan remot control RF yang digunakan untuk menggerakkan sebuah motor servo untuk akses membuka pintu ruangan tempat sensor *fingerprint* berada, kemudian data masukan sidik jari dari sensor fingerprint diatur oleh mikrokontroler untuk menggerakan kunci solenoid agar pintu utama brankas dapat terbuka.

Studi literatur yang berfokus pada pengontrolan akses sebuah ruangan dengan menggunakan berbagai teknologi biometrik sudah banyak dikembangkan. Makalah yang dipaparkan oleh (Aryani, Iskandar, & Indriyani, 2018) mengembangkan sebuah akses pintu ruangan berbasis voice recognition, dimana suara dari pengguna akan direkam oleh sebuah aplikasi di smartphone yang dikirimkan ke mikrokontroler melalui bluetooth. Disisi lain, (Nasir, 2016) mengembangkan sebuah sistem akses ruangan berbasis teknologi pengenalan wajah. Berdasarkan hasil pengujian, diperoleh bahwa sistem yang dibangun memiliki keakuratan yang cukup baik sebesar 87,80%.

Disamping penggunaan teknologi biometrik pengenalan suara dan wajah yang sudah dikembangkan oleh para peneliti, pengembangan sebuah akses ruangan menggunakan sidik jari adalah yang paling banyak digunakan. Dalam upaya untuk memperoleh sistem akses ruangan menggunakan sidik jari yang optimal, dilakukan berbagai modifikasi terhadap penelitian yang sudah ada sebelumnya. Modifikasi tersebut diantaranya adalah penggunaan mikrokontroler yang berbeda-beda, dari mulai jenis mikrokontroler ATMEGA328P (Saputra, Masud, Ramdhan, & Fitriani, 2014) (Sabar, Ismail, & Riyanto, 2017) sampai ke Arduino (Umam, 2018) (Sinurat, 2019) (Adriansyah, 2019). Selain modifikasi pada mikrokontroler juga dilakukan pengembangan terhadap fitur-fitur pada sistem akses ruangan berbasis sidik jari, seperti notifikasi terhadap admin ataupun perekaman data user yang keluar masuk ruangan. Hal ini membuat sistem akses ruangan menggunakan sidik jari masih memiliki peluang untuk dikembangkan dengan fitur-fitur tambahan serta jenis studi kasus ruangan yang akan diaksesnya.

Berbagai penelitian di atas menunjukan kelayakan teknologi biometrik sebagai teknologi untuk membatasi akses suatu area. Teknologi ini juga terbukti bisa dikombinasikan dengan berbagai perangkat dan teknik pengelolaan selanjutnya termasuk untuk monitoring pada kondisi WFH. Sistem keamanan dengan menggunakan sensor sidik jari dapat mengamankan ruangan dengan akses terbatas. Penggunaan kontroler mikrokontroler membuat sistem keamanan menjadi kompak dan sederhana.

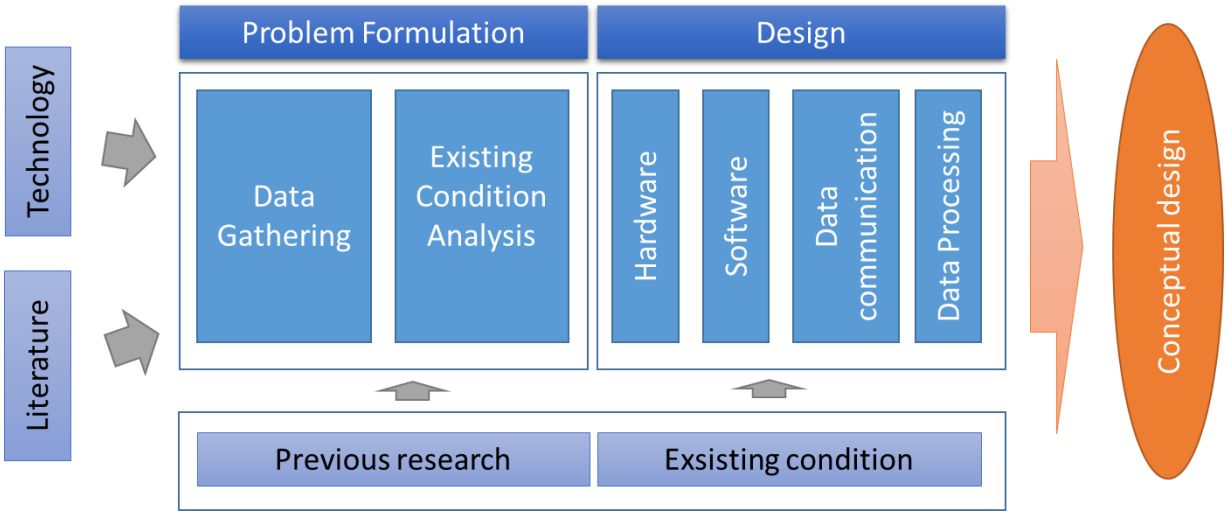
Berdasarkan studi literatur yang sudah dipaparkan sebelumnya, perlu dilakukan pengembangan atau modifikasi terhadap sistem yang sudah ada. Dengan mempertimbangkan kondisi yang ada di UIN Sunan Gunung Djati Bandung dan berbagai tinjauan teknologi yang ada, perlu dibuat sebuah desain konseptual sistem pengamanan area laboratorium dengan teknologi biometrik dan monitoringnya berbasis IoT dan *cloud system* dengan menggunakan sistem hybrid yang menggabungkan beberapa sistem biometric dilengkapi dengan fiur CCTV. Sehingga, dengan menggunakan sistem hybrid seperti itu diharapkan mampu meningkatkan keamanan laboratorium. Oleh karena itu, pada makalah ini akan dipaparkan desain konseptual sistem akses dan monitoring laboratorium yang lebih komprehensif, dan mendukung kondisi WFH yang dihadapi saat ini.

2 Metodologi

Penyusunan model dan desain konseptual sistem pembatasan akses laboratorium berbasis teknologi biometrik dan monitoringnya secara jarak jauh berbasis IoT yang dapat mendukung kondisi *Work From Home* (WFH),

dilakukan dengan studi literatur terhadap berbagai teknologi dan kondisi yang ada. Metodenya merupakan sebagian dari metode *engineering*, tetapi belum sampai pada tahap implementasi dan pengujian lapangan. Desain difokuskan pada kondisi di lingkungan UIN Sunan Gunung Djati Bandung.

Desain yang dilakukan mempertimbangkan beberapa aspek yaitu kondisi lingkungan UIN Sunan Gunung Djati Bandung, kondisi teknologi yang ada dan mungkin digunakan, perkembangan penelitian yang sudah ada, serta studi terhadap berbagai literatur lainnya. Desain yang dilakukan mencakup aspek perangkat keras, perangkat lunak, sistem komunikasi, dan sistem pengolahan data. Jika diskemakan, pendekatan yang digunakan dapat dilihat pada Gambar 1 berikut.



Gambar 1. Pendekatan penulisan makalah

3 Hasil dan Pembahasan

3.1 Kondisi Eksisting

Kondisi eksisting harus diperhitungkan dalam mendesain sistem, sehingga implementasinya lebih efisien. Tabel 1 menunjukkan gambaran singkat mengenai kondisi eksisting yang ada.

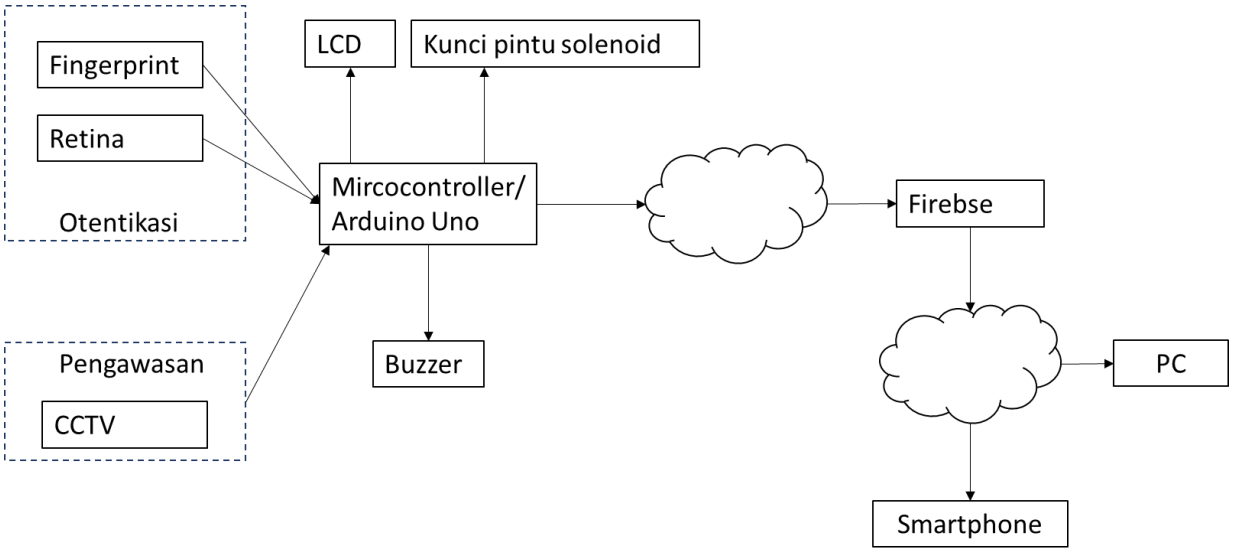
Tabel 1. Kondisi Eksisting

No.	Aspek	Kondisi
1	Teknologi *sensing* dan otentikasi	Saat ini UIN sudah memiliki teknologi *sensing* untuk akuisisi data dan otentikasi dengan perangkat *fingerprint* dan retina. Perangkat ini sudah ditempatkan di semua unit yang ada.
2	Teknologi pengawasan	UIN sudah memiliki *tools* untuk pengawasan keamanan dengan CCTV yang terpasang di setiap gedung dan ruangan, termasuk Laboratorium
3	Teknologi komunikasi dan telekomunikasi	UIN Bandung sudah memiliki daya dukung konektivitas yang baik dengan kecepatan 1 Gbps dan didukung infrastruktur di dalam area kampus dengan *fiber optic*
4	Teknologi server	Untuk mendukung layanan IT yang memadai, Uin sudah memiliki dukungan teknologi server terkini yang dikelola oleh PTIPD.

Kondisi teknologi yang ada di UIN cukup memadai untuk menjadi dasar pengembangan model sistem otentikasi laboratorium dan monitoring berbasis IoT.

3.2 Skema Sistem

Dengan memperhatikan berbagai kondisi yang ada, sistem yang diusulkan secara umum dapat dilihat pada Gambar 2.



Gambar 2. Skema sistem

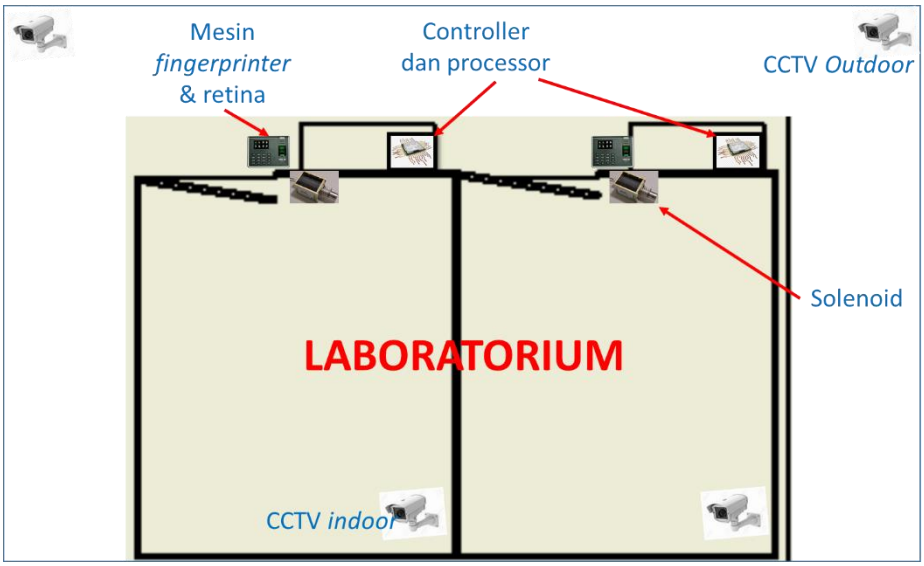
Proses otentikasi dapat dilakukan dengan memanfaatkan salah satu teknologi yang saat ini ada di UIN Sunan Gunung Djati, yaitu *fingerprint* dan retina. Teknologi ini juga diyakini memberikan akurasi yang tinggi, sebagaimana hasil riset yang disampaikan oleh NIST (NIST, 2003) bahwa *fingerprint* memberikan *false positive rate* sebesar 0.01% dengan akurasi 98.6 %. Sementara itu, iris memiliki akurasi 90-99 % tetapi mampu melakukan pengambilan data lebih cepat daripada fingerprint. Iris juga tidak terlalu dipengaruhi keadaan seperti halnya *finger* yang bisa basah, kering, berminyak, rusak, dan lain-lain.

Input otentikasi akan diproses oleh *microcontroller* untuk dicocokan dengan *database* yang telah tersimpan. Jika otentikasi diterima, maka microcontroller akan men-*triger* kunci pintu solenoid untuk membuka pintu laboratorium serta menampilkan informasi otetikasi pada layar LCD. Jika otentikasi ditolak, maka *microcontroller* akan menyalakan *buzzer* sebagai peringatan. Selain otentikasi *fingerprint* atau retina, sistem keamanan laboratorium juga didukung dengan skema pengawasan lingkungan menggunakan CCTV untuk merekam setiap pengguna yang mengakses laboratorium.

Semua informasi yang masuk ke microcontroller akan dikirimkan dan disimpan pada *cloud* firebase. Informasi yang disimpan pada *cloud* firebase yaitu pengguna yang terontetikasi ataupun tidak terontetikasi, waktu akses, dan wajah pengguna. Penanggung jawab laboratorium dapat melihat semua pengakses laboratorium melalui aplikasi *smartphone* atau *website* di PC. Untuk membatasi pengguna aplikasi atau *website*, digunakan otentikasi *username* dan *password*.

3.3 Desain Perangkat Keras dan Skema Prototipe Ruang

Perangkat keras didesain dengan memperhatikan kebutuhan otentikasi dan pengawasan. Skema penempatan perangkat dapat diilustrasikan pada Gambar 3.



Gambar 3. Ilustrasi penempatan perangkat

Komponen perangkat yang diperlukan untuk tiap node dapat dilihat pada Tabel 2.

Tabel 2. Komponen-komponen rangkaian elektronik sistem keamanan laboratorium

No	Komponen	Jumlah
1	ZFM-20	2
2	LCD 2C	2
3	Arduino Uno	1
4	ESP8266 NodeMCU	1
5	Buzzer	2
6	Solenoid	2
7	Relay	1
8	Catu daya	1
9	Regulator	1

3.4 Desain Perangkat Lunak

Perangkat lunak yang dikembangkan perlu memperhatikan aspek kebutuhan. Berdasarkan kondisi yang ada maka diperkukan sistem aplikasi yang dikembangkan berbasis Web dan dapat diakses melalui PC maupun samrtphone. Kebutuhan Fungsionalitas dan Non Fungsionalitas sistem secara keseluruhan dapat dilihat pada Tabel 3 dan Tabel 4.

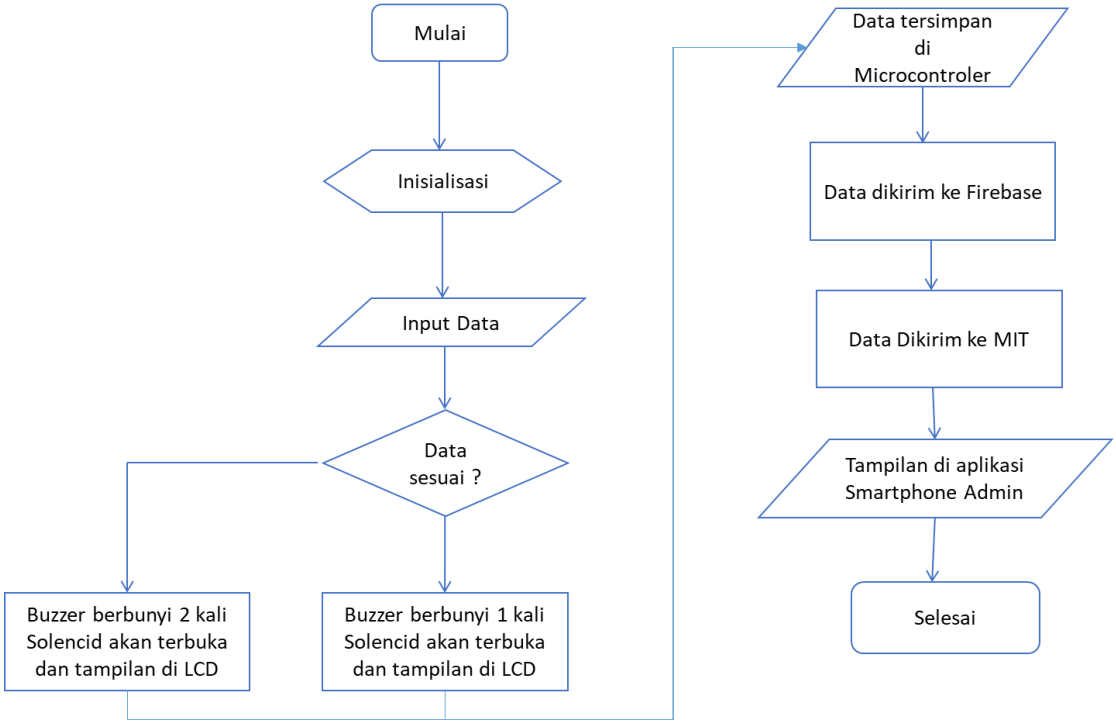
Tabel 3. Fungsionalitas sistem

No	Fungsionalitas	Keterangan
1	Login	Fungsi untuk login pengelola.
2	Registrasi	Fungsi untuk registrasi pengguna, baik registrasi dan akuisisi data melalui sidik jari maupun retina.
3	Data acquisition	Fungsi untuk akuisisi data ketika enrollment maupun pada saat implementasi.
4	Fungsi pemrosesan data	Mencakup kompresi dan pembacaan data
5	Fungsi komunikasi	Fungsi untuk komunikasi data. Fungsi ini didukung dengan ketersediaan konektivitas.
6	Fungsi dashboard	Menampilkan hasil pengolahan.

Tabel 4. Non Fungsionalitas sistem

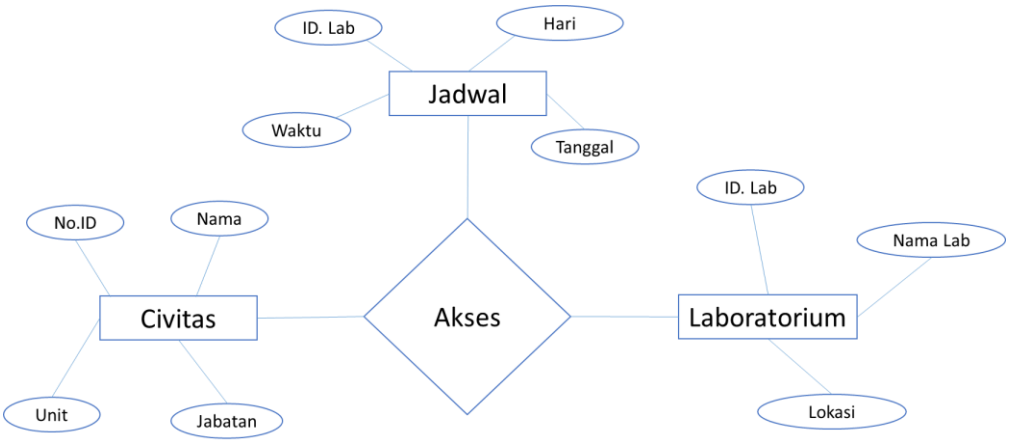
No	Non Fungsionalitas	Keterangan
1	Security	Sistem hanya bisa diakses oleh pengguna yang sah, data yang dikomunikasikan terenkripsi.
2	Availability	Tingkat ketersediaan sistem 98%.
3	Connectivity	Sistem senantiasa terhubung.
4	Readibility	Data harus dapat dibaca.
5	Reliability	Sistem harus tetap tersedia walaupun listrik mati minimal selama 1 jam.
6	Maintainability	Sistem dapat dipantau dari jarak jauh, dan aplikasi menyediakan CMS.
7	Performance	Sistem harus mampu melayani transaksi minimal 1000 per hari.
8	Interface	Tersedia dalam bahasa Indonesia dan Inggris, serta penataan menu yang baik.

Sementara itu, gambaran mengenai proses yang terjadi dalam sistem keamanan dapat dilihat pada *flowchart* program pada Gambar 4.



Gambar 4. Flow chart program sistem keamanan laboratorium

Sementara itu, database yang ada minimal memuat Tabel Pengguna/Sivitas Akademik UIN, Tabel Jadwal, Tabel Laboratorium dan Tabel Akses. Keterkaitan antar tabel-tabel tersebut dapat digambarkan dalam ER-Diagram sederhana pada Gambar 5.



Gambar 5. *ER-Diagram*

3.5 Desain Komunikasi Data

Informasi yang direkam oleh *microcontroller* akan dikirimkan ke *cloud* firebase menggunakan protokol *Hypertext Transfer Protocol Secure* (HTTPS) begitu juga dari *cloud* firebase ke *smartphone* atau PC menggunakan HTTPS. *Cloud* firebase akan bertindak sebagai *server* sementara *microcontroller* dan *smartphone* atau PC sebagai *client*. HTTPS merupakan pengembangan dari protokol *Hypertext Transfer Protocol* (HTTP) yang ditambahkan kemampuan enkripsi pada informasi yang dibawanya sehingga tidak mudah dibaca oleh orang yang tidak berkepentingan. Metode enkripsi data pada HTTPS menggunakan protokol *Transport Layer Security* (TLS) atau *Secure Socket Layer* (SSL). Dalam melakukan enkripsi pada protokol HTTPS memerlukan autentikasi antara *client* dan *server* menggunakan sertifikat digital. HTTPS menggunakan *port* 443 sebagai alamat komunikasi pada layer aplikasi. Semua aturan tentang HTTPS didokumentasi pada RFC2818.

4 Kesimpulan

Berdasarkan paparan yang sudah dijelaskan sebelumnya, dapat disimpulkan bahwa sistem akses laaboratorium yang akan dibangun memiliki fitur keamanan yang komprehensif. Fitur-fitur tersebut diantaranya akses laboratorium yang dibangun berbasis sistem biometric sidik jari dan retina, fitur pengawasan CCTV, serta sistem monitoring akses keluar masuk laboratorium yang dapat diakses melalui smartphone ataupun PC kapan saja dan dimana saja. Selain dari itu, diharapkan desain konseptual tentang pengembangan sistem akses laboratorium berbasis sidik jari ini mampu menghasilkan sistem keamanan yang lebih optimal dan dapat diterapkan pada kondisi pandemic yang saat ini dirasakan. Sehingga pengontrolan laboratorium dapat diakses dari rumah, sehingga menunjang program pemerintah yaitu Work from Home (WFH) yang saat ini sedang dilakukan di Indonesia.

Referensi

Adriansyah, M. (2019). *Sistem Keamanan Pintu Otomatis Pada Lobi Jurusan Teknik Komputer Menggunakan Sensor Fingerprint Berbasis Mikrokontroler Arduino (Diploma Thesis)*. Palembang: Politeknik Negeri Sriwijaya.

Aryani, D., Iskandar, D., & Indriyani, F. (2018). Perancangan Smart Door Lock Menggunakan Voice Recognition Berbasis Rapberry Pi 3. *Jurnal Cerita, 4*(2), 180-189.

Asror, I., & Siradj, Y. (2016). Desain dan Implementasi Sistem CCTV Menggunakan Cloud. *TELEKONTRAN, 4*(1), 53-58.

Dewa, E. P., & Kartadie, R. (2016). Integrasi Sensor Gerak Dan Ponsel Pada Arduino Sebagai Sistem Kontrol Keamanan Rumah. *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika, 1*(2), 30-37.

FA, A. C., & P, B. H. (2016). *Sistem Pengaman Brankas Menggunakan Sensor Fingerprint Dan Remot Kontrol RF Berbasis Arduino Uno (Diploma thesis).* Surakarta: Universitas Muhamadiyah Surakarta.

Gunawan, T. S., Yaldi, I. R., Kartiwi, M., Ismail, N., Za'bah, N. F., Mansor, H., & Nordin, A. N. (2017). Prototype design of smart home system using internet of things. *Indonesian Journal of Electrical Engineering and Computer Science, 7*(1), 107-115.

Haryanto, B., Ismail, N., & Pristianto, E. J. (2018). Sistem Monitoring Suhu dan Kelembapan secara Nirkabel pada Budidaya Tanaman Hidroponik. *Jurnal Teknologi Rekayasa, 3*(1), 47-54.

Hill, C. (2015). Wearables – the future of biometric technology? *Elsevier: Biometric Technology Today, 2015*(8), 5-9.

Kamelia, L., S.R, A. N., W.S, M. S., & Mulyana, E. (2014). Door-Automation System Using Bluetooth-Based Android For Mobile Phone. *ARPN Journal of Engineering and Applied Sciences, 9*(10), 1759-1762.

Kresnha, P. E., Susilowati, E., & Mujiastuti, R. (2018). Pengembangan Sistem Keamanan Rumah Indoor Efisien Berbasis Human Detection Menggunakan CCTV Dan SMS Gateway. *Seminar Nasional Pendidikan Teknik Informatika (SENAPATI)* (pp. 233-239). Denpasar: Universitas Pendidikan Ganesha.

Nasir, A. (2016). Perancangan Aplikasi Pengenalan Wajah Sebagai Media Akses Kontrol Pada Organisasi XYZ. *Jurnal Edukasi dan Penelitian Informatika (JEPIN), 2*(1), 71-77.

NIST. (2003). *Biometric Accuracy Standards.* NIST.

Pasha, A. K., Mulyana, E., Hidayat, C., Ramdhani, M. A., Kurahman, O. T., & Adhipradana, M. (2018). System Design of Controlling and Monitoring on Aquaponic Based on Internet of Things. *4th International Conference on Wireless and Telematics (ICWT).* Nusa Dua: IEEE.

Sabar, M., Ismail, K., & Riyanto, S. (2017). Rancang Bangun Sistem Akses Kontrol Keluar Masuk Rumah Menggunakan Selenoid Doorlock Dan Sensor Fingerprint Berbasis Mikrokotroler Atmega 328. *CITISEE* (pp. 335-338). Purwokerto: AMIK Purwokerto.

Saputra, D., Masud, A. H., Ramdhan, M., & Fitriani, D. (2014). Akses control ruangan menggunakan sensor sidik jari berbasis mikrokontroler atmega328p. *Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA), 2*, pp. 596-604,. Yogyakarta.

Sinurat, D. (2019). *Akses Kontrol Ruangan Menggunakan Sensor Sidikjari (Fingerprint ZFM-20) Berbasis Arduino (Diploma Thesis).* Medan: Universitas Sumatera Utara.

Siswanto, A., Efendi, A., & Yulianti, A. (2018). Alat Kontrol Akses Pintu Rumah Dengan Teknologi Sidik Jari Di Lingkungan Rumah Pintar Dengan Data Yang Di Enkripsi. *Jurnal Penelitian Pos dan Informatika, 8*(2), 97-107.

Syahidulhaq, H. A., Hafiddudin, & Aulia, S. (2016). Sistem Keamanan Berbasis Alarm IP Camera dengan Passive Infrared Receiver (PIR) Sensor dan SMS Gateway. *Jurnal Elektro dan Telekomunikasi Terapan (JETT), 3*(2), 312-320.

Tobing, S. L. (2014). Rancang Bangun Pengaman Pintu Menggunakan Sidik Jari (Fingerprint) Dan Smartphone Android Berbasis Mikrokontroler Atmega8. *Jurnal Teknik Elektro Universitas Tanjungpura, 1*(1), 1-7.

Umam, M. K. (2018). *Rancang Bangun Akses Kendali Pintu Menggunakan Sensor Fingerprint (Sidik Jari) Berbasis Arduino Uno (diploma thesis).* Kudus: Universitas Muria.

Usman, Rahmansyah, A. A., & Apriadi, N. F. (2017). Rancang Bangun Pagar Otomatis dengan Finger Print Berbasis Mikrokontroller. *Jurnal Teknologi Terapan, 3*(1), 35-41.

Biografi Penulis

Nama : Rina Mardiati
NIP : 198409042009122002
Pendidikan : S3 Teknik Elektro ITB
Pangkat/Jabatan : Penata Tk. I/ III/d
Fungsional : Lektor
Unit : Jurusan Teknik Elektro, Fakultas Saintek, UIN SGD Bandung

Nama : Nanang Ismail
NIP : 197505262011011002
Pendidikan : S2 Teknik Elektro ITB
Pangkat/Jabatan : Penata Tk. I/ III/d
Fungsional : Lektor
Unit : Jurusan Teknik Elektro, Fakultas Saintek, UIN SGD Bandung

Nama : Adam Faroqi
NIP : 1974051620091210001
Pendidikan : S2 Teknik Industri
Pangkat/Jabatan : Pembina IV/a
Fungsional : Lektor Kepala
Unit : Jurusan Teknik Elektro, Fakultas Saintek, UIN SGD Bandung

Nama : Mufid Ridlo Effendi
NIP : 198304212016033043
Pendidikan : S2 Teknik Elektro ITB
Pangkat/Jabatan : III/b
Fungsional : Tenaga Pendidik
Unit : Jurusan Teknik Elektro, Fakultas Saintek, UIN SGD Bandung