|  |  |
| --- | --- |
|  | UNIVERSITAS DIPONEGORO – FAKULTAS TEKNIK  DEPARTEMEN TEKNIK ELEKTRO  *Jl. Prof. H. Soedarto, SH, Tembalang, Semarang 50275*  *Telp/Faks. (024)-7460057 e-mail: departemen@elektro.undip.ac.id* |

**Dokumen Pengembangan Produk**

Lembar Sampul Dokumen

|  |  |  |
| --- | --- | --- |
| Judul Dokumen | **TUGAS AKHIR:**  **Rancang Bangun Sistem Keamanan Kunci Pintu GedungBerbasis *Internet of Things*** | |
|  |  | |
| Jenis Dokumen | **SPESIFIKASI** | |
|  | Catatan: Dokumen ini dikendalikan penyebarannya oleh Dept. Teknik Elektro Undip | |
| Nomor Dokumen | **B200-01-TA2223.2.19012** | |
|  |  | |
| Nomor Revisi | **01** | |
|  |  | |
| Nama File | **B200-2-TA2223** | |
|  |  | |
| Tanggal Penerbitan | **6 Februari 2023** | |
|  |  | |
| Unit Penerbit | **Departemen Teknik Elektro Undip** | |
|  |  | |
| Jumlah Halaman | **25** | (termasuk lembar sampul ini) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Pengusul | | | | |
| Pengusul | Nama  NIM | **Henric Dhiki Wicaksono**  21060119120011 | Jabatan  Tanda Tangan | Anggota |
|  | Nama  NIM | **Novi Dianasari**  21060119120039 | Jabatan  Tanda Tangan | Anggota |
|  | Nama  NIM | **Muhammad Khoiril Wafi**  21060119140133 | Jabatan  Tanda Tangan | Anggota |
| Pembimbing | Nama | **M. Arfan, S.Kom., M.Eng.** | Tanda Tangan |  |
| Utama | NIP | 198408172015041002 |  |  |
| Pendamping | Nama | **Imam Santoso, S.T., M.T.** | Tanda Tangan |  |
|  | NIP | 197012031997021001 |  |  |

**DAFTAR ISI**

[1 PENDAHULUAN 4](#_Toc104882779)

[1.1 Ringkasan Isi Dokumen 4](#_Toc104882780)

[1.2 Aplikasi Dokumen 4](#_Toc104882781)

[1.3 Referensi 5](#_Toc104882782)

[1.4 Daftar Singkatan 5](#_Toc104882783)

[2 SPESIFIKASI 6](#_Toc104882784)

[2.1 Definisi, Fungsi, dan Spesifikasi dari Solusi 6](#_Toc104882785)

[2.1.1 Definisi 6](#_Toc104882786)

[2.1.2 Fungsi 7](#_Toc104882787)

[2.1.3 Spesifikasi 7](#_Toc104882788)

[2.2 Spesifikasi Produk 10](#_Toc104882789)

[2.3 Penjelasan Fungsi, Fitur, dan Verifikasi 12](#_Toc104882790)

[2.4 Biaya dan Jadwal 21](#_Toc104882791)

[3 PENUTUP 23](#_Toc104882792)

# Catatan Sejarah Perbaikan Dokumen

|  |  |
| --- | --- |
| **VERSI, TGL, OLEH** | **PERBAIKAN** |
| 01,  7 April 2023,  oleh Henric Dhiki Wicaksono, Novi Dianasari  dan Muhammad Khoiril Wafi. | *Draft* Dokumen B200 |

1. PENDAHULUAN

## **Ringkasan Isi Dokumen**

Dokumen ini berisikan uraian spesifikasi produk Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* (IoT). Dokumen ini menjelaskan tentang sebuah sistem yang menggunakan teknologi IoT untuk mengatur pengelolaan kunci pintu gedung serta melakukan pemantauan secara *remote* melalui jaringan internet. Definisi sistem menjelaskan permasalahan yang menjadi dasar dan alasan untuk melakukan rancang bangun sistem. Fungsi sistem menjelaskan kegunaan sistem. Spesifikasi sistem menjelaskan rincian seluruh subsistem produk secara umum.

Pada dokumen B200 ini akan dijelaskan desain sistem yang terdiri dari penjelasan setiap subsistem yang dibuat. Subsistem pertama adalah perancangan sistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT. Subsistem kedua adalah perancangan aplikasi *mobile* dan *website* sebagai antarmuka pengguna. Subsistem ketiga adalah perancangan sistem *database* dan *server* serta sistem keamanan kunci pintu gedung dengan *access control* sebagai pusat penyimpanan data dan kendali sistem keamanan kunci pintu gedung. B200 ini selanjutnya digunakan sebagai acuan dalam pelaksanaan proyek dan pengerjaan produk Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* (IoT).

## **Aplikasi Dokumen**

Dokumen ini digunakan dalam proses pengembangan produk Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* (IoT) untuk:

1. Sebagai gambaran spesifikasi perancangan produk, implementasi, dan pengujian produk pada tahap selanjutnya.
2. Menjelaskan tahap verifikasi produk dalam menguji fungsionalitas dan non-fungsional dari keseluruhan subsistem dengan biaya dan jadwal kerja pembuatan produk.
3. Menjadi catatan proses dan revisi yang dikerjakan.

Dokumen B200 ini diajukan kepada dosen pembimbing tugas akhir dan tim tugas akhir Program Studi Sarjana Teknik Elektro Undip sebagai bahan penilaian tugas akhir.

## **Referensi**

[1] A. T. Sianturi, “RANCANG BANGUN SISTEM KEAMANAN RUANGAN DENGAN SENSOR CAHAYA BERBASIS ARDUINO UNO MENGGUNAKAN SMS GATEWAY,” Universitas Sumatra Utara, Medan, 2019. Accessed: Jan. 19, 2023. [Online]. Available: https://123dok.com/document/zpnl36v4-rancang-keamanan-ruangan-berbasis-arduino-menggunakan-gateway-laporan.html

## **Daftar Singkatan**

**Tabel 1.1** Daftar Singkatan

| Singkatan | Arti |
| --- | --- |
| IoT | *Internet of Things* |
| Wi-Fi | *Wireless Fidelity* |
| SQL | *Structured Query Language* |
| FCM | *Firebase Cloud Messaging* |
| HTTPS | *Hypertext Transfer Protocol Secure* |
| iOS | *iPhone Operating System* |
| PC | *Personal Computer* |
| ESP | *Espressif* |
| IDE | *Integrated Development Environment* |
| PCB | *Printed Circuit Board* |
| UI | *User Interface* |
| XSS | *Cross-Site Scripting* |
| QR-*Code* | *Quick Response Code* |
| URL | *Uniform Resource Locator* |
| SSL/TLS | *Secure Sockets Layer/Transport Layer Security* |

1. SPESIFIKASI PRODUK

## **Definisi**

Sistem keamanan merupakan aspek penting untuk mendukung kinerja sebuah gedung. Gedung itu memiliki beberapa ruangan dan beberapa pintu untuk masuk[1]. Gedung pasti memiliki cara tersendiri dalam menjaga privasi dan keamanan setiap ruangnya. Dengan sistem kontrol akses, pemilik gedung dan properti dapat melakukan lebih dari sekadar mengontrol akses ke area yang dilindungi. Sistem ini juga dapat dilakukan secara elektronik dengan membuat catatan sejarah atau informasi tentang setiap orang yang memasuki ruangan. Catatan ini membantu pengelolan dalam mengidentifikasi siapa yang memasuki ruangan pada waktu tertentu.

*Internet of Things* (IoT) adalah sebuah konsep yang bertujuan untuk terus memperluas manfaat dari koneksi internet dengan menggunakan beberapa perangkat seperti sensor dan aktutor yang terhubung menjadi sebuah jaringan. *Internet of Things* (IoT) bisa dimanfaatkan dalam berbagai hal untuk mempermudah aktifitas manusia, salahsatunya yaitu pada gedung perkantoran maupun rumah sebagai alat untuk mengendalikan peralatan elektronik dan juga sebagai suatu sistem keamanan yang dapat dioperasikan dari jarak jauh melalui koneksi internet.

Pada saat ini proses pengelolaan kunci pintu gedung masih menggunakan metode manual dengan menggunakan kunci fisik yang banyak sehingga tidak efisien. Oleh karena itu dibangunlah sistem keamanan kunci pintu gedung berbasis IoT yang merupakan sebuah sistem yang menggunakan teknologi IoT untuk memastikan keamanan gedung dan memudahkan pengelolaan akses pintu. Sistem ini terdiri dari perangkat keras dan perangkat lunak yang terintegrasi dan bekerja bersama-sama untuk memantau dan mengatur akses pintu gedung. Misalnya, dengan menggunakan *website* seorang operator dapat mengatur siapa yang diijinkan untuk mengakses ruangan tertentu serta memantau kondisi pintu secara *real-time* melalui jaringan internet. Penggunaan aplikasi *mobile* juga memudahkan pengguna dalam mengakses ruangan dengan menggunakan prangkat *smartphone* yang *compact*. Sistem keamanan kunci pintu gedung berbasis IoT juga menjamin keamanan gedung dengan solusi teknologi yang inovatif.

### **Fungsi**

Produk "Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*" memiliki beberapa fungsi berikut ini:

1. Merancang sistem komunikasi data dua arah dan perangkat penguncian yang digunakan untuk mendukung knerja dari sistem keamanan kunci pintu gedung berbasis IoT.
2. Merancang sistem *database* dan *serve*r sebagai pusat penyimpanan data dan pengendalian sistem keamanan kunci pintu gedung serta merancang mekanisme *access control* sebagai metode penguncian.
3. Merancang aplikasi *mobile* sebagai pirantiakses masuk pintu gedung dan *website* untuk mendukung pengelolaan kunci pintu gedung.

### **Spesifikasi**

Berdasarkan fungsi-fungsi yang dimiliki, produk “Rancang BangunSistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*” memiliki spesifikasi sebagai berikut:

1. Spesifikasi subsistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT.
   1. Spesifikasi subsistem komunikasi data dua arah:

* Protokol Komunikasi: Sistem komunikasi data dua arah harus menggunakan protokol yang handal dan aman untuk mentransfer data antara perangkat penguncian pintu dan *server* pusat. Beberapa protokol yang dapat digunakan adalah HTTPS.
* Pengenkripsian Data: Untuk menjaga keamanan data yang ditransfer antara perangkat penguncian pintu dan *server*, subsistem komunikasi harus menyediakan enkripsi data yang handal dan aman. Beberapa teknologi enkripsi yang dapat digunakan adalah SSL/TLS.
* Pengiriman Data *Real-time*: Sistem komunikasi data dua arah harus mampu mentransfer data secara *real-time* antara perangkat penguncian pintu dan *server* pusat dan sebaliknya. Hal ini penting untuk memastikan bahwa penguncian pintu gedung dapat dilakukan secara cepat dan akurat.
* *Monitoring* dan Notifikasi: Sistem komunikasi data dua arah harus memiliki fitur *monitoring* dan notifikasi yang dapat memberikan informasi tentang status penguncian pintu, kondisi perangkat penguncian, dan aktivitas penggunaan pintu gedung. Notifikasi dapat dikirim melalui aplikasi *mobile* dan *website.*
  1. Spesifikasi perangkat penguncian:
* Kompatibilitas IoT: Perangkat penguncian harus mendukung teknologi IoT, sehingga dapat terhubung dengan jaringan internet dan sistem keamanan yang berbasis IoT.
* Pengendalian Akses: Perangkat penguncian harus memiliki fitur pengendalian akses yang dapat diatur sesuai dengan kebijakan keamanan pintu gedung. Fitur ini dapat diatur melalui *website*.
* Keamanan Fisik: Perangkat penguncian harus dirancang dengan keamanan fisik yang baik, sehingga sulit untuk dibobol atau dirusak oleh pihak yang tidak berwenang. Perangkat penguncian juga harus tahan terhadap kondisi lingkungan yang ekstrem seperti suhu yang tinggi atau rendah, kelembaban yang tinggi, dan debu.

Dengan mengikuti spesifikasi tersebut, subsistem komunikasi data dua arah dan perangkat penguncian dapat bekerja dengan baik dan dapat memberikan sistem keamanan yang handal dan aman untuk pengguna pintu gedung berbasis IoT.

1. Spesifikasi subsistem *database* dan *serve*r serta sistem keamanan kunci pintu gedung dengan *Access Control*.
2. Spesifikasi subsistem *database*.

* Pengolahan Data: sistem *database* harus mampu melakukan pengolahan data secara cepat dan efisien untuk menjamin ketersediaan data.
* Kapasitas: sistem *database* harus mampu menyediakan tempat penyimpanan yang cukup untuk menyimpan data seperti data pengguna, data pintu, data gedung dan lain sebagainya.
* Keamanan: sistem *database* harus memiliki sistem keamanan yang dapat melindungi akses data didalam *database* dan pengguna dari luar tidak diijinkan untuk mengakses *database* secara langsung.

1. Spesifikasi subsistem *server*:

* Ketersediaan: *server* yang dirancang harus dapat bekerja secara terus-menerus untuk menyediakan layanan bagi pengguna, *server* juga harus mampu menangani permintaan pengguna secara bersamaan dengan waktu respin yang cepat.
* Keamanan: *server* harus menerapkan mekanisme keamanan dari segi komunikasi data maupun pengelolaan server. penggunan *firewall* serta komunikasi terenkripsi sangat diperlukan dalam implementasi server.

1. Spesifikasi subsistem keamanan kunci pintu gedung dengan *Access Control*:

* Fitur Akses Kontrol: Sistem keamanan kunci pintu gedung harus memiliki fitur akses kontrol yang dapat diatur secara *realtime* sesuai dengan kebijakan keamanan pintu gedung, seperti pembatasan akses berdasarkan waktu atau lokasi.
* Riwayat Aktifitas: Sistem keamanan kunci pintu gedung harus dapat menyimpan catatan riwayat aktifitas setiap pengguna.
* Kendali Jarak Jauh: Sistem keamanan kunci pintu gedung menyediakan metode untuk membuka pintu secara *remote* melalui koneksi internet.
* Notifikasi: Sistem keamanan kunci pintu gedung dapat memeberikan notifikasi terkait dengan status pintu secara realtime. Jika terjadi perubahan status atau terjadi penerobosan maka sistem akan memberikan notifikasi ke pengelola gedung.
* Penjadwalan: sistem keamanan kunci pintu gedung menyediakan fitur untuk membuka kunci pintu secara terjadwal. Fitur ini bisa diaplikasikan untuk ruangan yang dapat diakses oleh pengunjung umum tapi dalam rentang waktu tertentu setiap harinya.

Dengan mengikuti spesifikasi tersebut, subsistem *database* dan *server* serta sistem keamanan kunci pintu gedung dengan *Access Control* dapat bekerja dengan baik dan dapat memberikan sistem keamanan yang handal dan aman untuk pengguna pintu gedung.

1. Spesifikasi aplikasi *mobile* sebagai pirantiakses masuk pintu gedung dan *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh.
2. Spesifikasi aplikasi *mobile* sebagai piranti akses masuk pintu gedung:

* Sistem Operasi: Aplikasi *mobile* yang dikembangkan harus dapat digunakan pada perangkat mobile android dari berbagai merek dan versi.
* Fitur Keamanan: Aplikasi mobile yang dikembangkan memiliki mekanisme autentikasi keamanan untuk memastikan hanya pengguna yang terdaftar yang dapat membuka pintu gedung.
* Koneksi Internet: Aplikasi *mobile* yang dikembangkan harus dapat terhubung dengan internet untuk mengakses sistem keamanan pintu gedung.
* Komunikasi Bluetooth: Aplikasi *mobile mobile* yang dikembangkan harus bisa berkomunikasi dengan perangkat kunci pintu dengan menggunakan bluetooth.

1. Spesifikasi *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh:

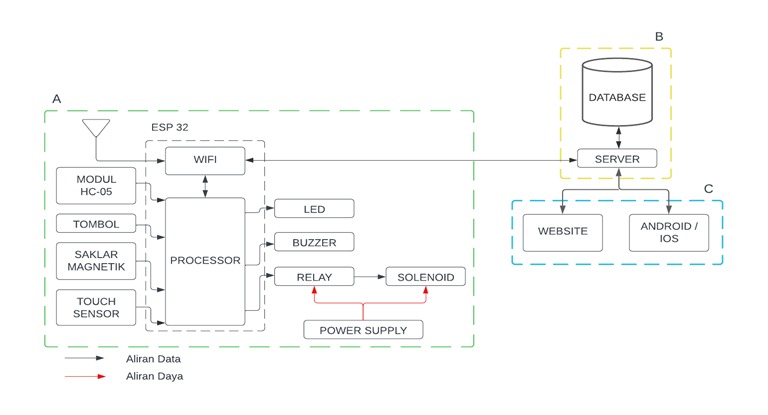
* *Platform*: *Website* harus menggunakan *platform* yang handal dan aman untuk memastikan keamanan data yang disimpan pada *website*.
* Fitur *Monitoring*: *Website* harus memiliki fitur *monitoring* yang dapat memberikan informasi tentang aktivitas penggunaan pintu gedung, seperti *log* aktivitas, siapa yang membuka pintu, dan kapan pintu dibuka.
* Fitur *Controlling*: *Website* harus memiliki fitur *controlling* yang memungkinkan pengelola untuk mengontrol akses ke pintu gedung dari jarak jauh, seperti membuka atau mengunci pintu gedung.
* Keamanan: *Website* harus dilengkapi dengan sistem keamanan yang ketat, seperti *firewall*, SSL/TLS, dan IDS/IPS, untuk melindungi data dan informasi penting yang tersimpan pada *website*.
* *User Interface*: *Website* harus memiliki *user interface* yang *user-friendly* dan mudah digunakan oleh pengguna.

Dengan mengikuti spesifikasi tersebut, perangkat *mobile* sebagai piranti akses masuk pintu gedung dan *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh dapat berfungsi dengan baik dan memberikan akses yang aman dan terkontrol untuk pengguna pintu gedung.

## **Spesifikasi Produk**

1. **Spesifikasi Sistem Berdasarkan Kemampuan dan Fungsionalitas**

Secara umum diagram blok utama sistem secara keseluruhan digambarkan pada Gambar 2.1.



**Gambar 2.1** Diagram Blok Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*

Diagram blok utama mengkombinasikan 3 subsistem yaitu subsistem komunikasi data dua arah dan perangkat penguncian pintu gedung berbasis IoT yang ditunjukkan pada bagian A Gambar 2.1, subsistem *server* dan *database* yaitu blok aliran data pada *server* yang ditunjukkan pada bagian B Gambar 2.1, sertasubsistem *user interface* yaitu blok antarmuka perangkat *mobile* berbasis android dan iOS serta *website* yang ditunjukkan pada bagian C Gambar 2.1.

Spesifikasi sistem keamanan kunci pintu gedung berbasis IoT memiliki beberapa kemampuan dan fungsi penting untuk memastikan keamanan dan efisiensi pengelolaan kunci pintu gedung. Salah satunya adalah akses kontrol, yaitu fitur pemantauan dan kontrol akses yang efektif seperti pengaturan hak akses pengguna, kontrol pintu dari jarak jauh, dan pemantauan kondisi pintu. Pengaturan akses sepenuhnya dilakukan didalam server, dengan menggunakan metode ini maka pengaturan hak akses penggunakan dapat dilakukan secara langsung dikarenakan pengguna akan selalu meminta kunci akses setiap kali akan mengakses suatu pintu. Penangannan permintaan kunci akses akan menjadi perhatian dalam pengembangan server dan database, keduanya harus dapat bekerja untuk menangani kemungkinan permintaan secara bersamaan dalam satu waktu. Sistem yang dikembangkan juga melakukan pencatatan riwayat aktifitas akses pengguna serta melakukan penjadwalan untuk setiap pintu. Sistem yang dikembangkan harus dapat menampung banyak pintu pada suatu gedung serta mampu untuk dikembangkan lebih lanjut untuk digunakan jumlah pintu atau jumlah gedung. Keamanan data juga harus terjamin dengan enkripsi data dan autentikasi yang kuat. Terakhir, sistem harus memiliki dukungan teknis yang memadai dan tersedia untuk memastikan solusi dapat digunakan dengan baik dan efisien.

## **Penjelasan Fungsi, Fitur, dan Verifikasi**

Pada subbab ini akan dijelaskan terkait fungsi, fitur, dan proses verifikasi atau pengujian sistem keamanan kunci pintu gedung berbasis *internet of things.* Berikut penjelasan fungsi yang dimiliki oleh produk tersebutmeliputi:

1. Merancang sistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT.

* Komunikasi data dua arah: memastikan komunikasi yang efektif dan tepat antara perangkat IoT dengan *server* dan antar perangkat dalam jaringan.
* Penguncian yang didukung: memastikan perangkat penguncian pintu yang terintegrasi dengan sistem IoT, sehingga pintu dapat dibuka dan ditutup dengan tepat dan efisian.
* Kontrol akses: memastikan bahwa hanya pengguna dengan hak akses yang sesuai yang dapat membuka pintu.
* Pencatatan akses*:* memastikan aktivitas pengguna pada setiap pintu tercatat dan dapat dianalisis.
* Notifikasi: memastikan bahwa pengelola atau pemilik gedung dapat menerima notifikasi saat terjadi aktivitas yang tidak diinginkan.
* Skalabilitas dan fleksibilitas: memastikan bahwa sistem dapat dikonfigurasi dan diperluas sesuai dengan kebutuhan, sehingga dapat memenuhi permintaan penambahan ruangan atau penambahan perangkat.

1. Merancang sistem *database* dan *serve*r serta sistem keamanan kunci pintu gedung dengan kontrol akses.

* Penyimpanan data: memastikan bahwa semua data yang terkait dengan sistem keamanan kunci pintu gedung dapat disimpan dan diakses secara efisien dan tepat waktu.
* *Server*: memastikan bahwa *server* dapat menangani beban akses dan pemrosesan data secara efisien dan handal.
* Sistem keamanan *database*: memastikan bahwa data yang disimpan aman dan terlindungi dari akses yang tidak sah.
* Kontrol akses: memastikan bahwa hanya pengguna dengan hak akses yang sesuai yang dapat membuka pintu.
* Notifikasi: memastikan bahwa admin atau pemilik gedung dapat menerima notifikasi saat terjadi aktivitas yang tidak diinginkan.
* Skalabilitas dan fleksibilitas: memastikan bahwa sistem dapat dikonfigurasi dan diperluas sesuai dengan kebutuhan, sehingga dapat memenuhi permintaan penambahan ruangan atau penambahan perangkat.

1. Merancang perangkat *mobile* sebagai pirantiakses masuk pintu gedung dan *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh.

* Akses pintu: memastikan bahwa pengguna dapat membuka pintu dengan menggunakan perangkat *mobile* seperti *smartphone* atau tablet.
* *Monitoring* dan *controlling* jarak jauh: memastikan bahwa pemilik bangunan atau admin dapat melakukan *monitoring* dan *controlling* sistem.

Untuk dapat menjalankan fungsi dari produk sistem keamanan kunci pintu gedung berbasis *internet of things,* sistem memiliki beberapa fitur. Fitur produk dijelaskan pada Tabel 2.1.

**Tabel 2.1** Fitur Produk Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*

|  |  |
| --- | --- |
| **Fitur Utama** | **Fitur Mendasar** |
| Produk sistem keamanan kunci pintu gedung berbasis *internet of things* memiliki kapabilitas untuk meningkatkan dalam hal keamanan untuk sistem kunci pintu gedung. | 1. Kendali Jarak Jauh   Proses pengaturan kunci pintu (*lock* dan *unlock*) dapat dilakukan dari jarak jauh. Pengendalian dapat dilakukan dengan menggunakan aplikasi *mobile* atau *website*. Kendali jarak jauh hanya bisa dilakukan oleh pengelola yang memiliki akses penuh atas sistem kunci pintu IoT.  Jadi, salah satu keuntungan utama dari desain sistem keamanan kunci pintu gedung berbasis IoT adalah kemampuan untuk mengontrol akses ke gedung secara *remote*. Dengan sistem ini, pihak yang berwenang (pengelola) dapat mengakses kunci pintu gedung melalui perangkat yang terhubung ke internet, seperti *smartphone* atau komputer, dan mengontrol akses ke gedung dari jarak jauh.  Ini memungkinkan pihak yang berwenang untuk memberikan atau mencabut akses ke gedung tanpa harus berada di lokasi gedung secara fisik. Ini bisa sangat bermanfaat dalam situasi di mana pihak yang berwenang tidak bisa datang ke gedung secara fisik, misalnya karena sedang berada di luar kota.  Selain itu, dengan mengontrol akses ke gedung secara *remote*, pihak yang berwenang juga dapat memantau aktivitas akses ke gedung secara *real-time* dan membuat laporan atas aktivitas tersebut. Ini memudahkan pengelolaan akses ke gedung dan membantu menjamin keamanan gedung.   1. Riwayat akses   Salah satu keuntungan menggunakan desain sistem keamanan kunci pintu gedung berbasis IoT adalah kemampuan untuk mencatat aktivitas akses pengguna. Dengan sistem ini, setiap kali seseorang membuka atau mengunci pintu, aktivitas tersebut akan tercatat dalam sistem dan dapat diakses oleh pihak yang berwenang. Ini memungkinkan pihak yang berwenang untuk memantau aktivitas akses ke gedung dan membuat laporan atas aktivitas tersebut.  Informasi yang biasanya dicatat dalam sistem keamanan kunci pintu gedung berbasis IoT termasuk tanggal dan waktu akses, informasi tentang orang yang melakukan akses. Informasi ini dapat bermanfaat untuk menganalisis pola akses ke gedung atau untuk membantu menyelidiki kejadian yang mungkin terjadi di gedung.   1. Kemudahan pengelolaan akses ke gedung   Desain sistem keamanan kunci pintu gedung berbasis IoT juga dapat memudahkan pengelolaan akses ke gedung. Dengan sistem ini, pihak yang berwenang dapat dengan mudah menambah atau menghapus akses ke gedung untuk individu tertentu. Misalnya, jika seseorang hendak memasuki gedung untuk pertama kalinya, pihak yang berwenang dapat dengan mudah menambahkan akses untuk orang tersebut ke dalam sistem. Begitu juga, jika seseorang tidak lagi memerlukan akses ke gedung, pihak yang berwenang dapat dengan mudah menghapus akses untuk orang tersebut dari sistem. Ini memudahkan pengelolaan akses ke gedung karena pihak yang berwenang tidak perlu mengeluarkan atau mengganti kunci fisik setiap kali ada perubahan dalam akses ke gedung.   1. Pengawasan   Setiap perangkat penguncian pintu akan mengawasi kondisi pintu setiap saat. Jika pintu terbuka secara tidak normal, maka sistem akan memberikan notifikasi peringatan bahwa ada pintu yang terbuka dan dimungkinkan adanya indikasi penerobosan. Jadi, sistem ini dapat memantau aktivitas pintu secara *real-time* serta memberikan notifikasi kepada pengelola jika terjadi aktivitas yang tidak diinginkan di pintu.   1. Penjadwalan   Sistem yang dibuat memungkinkan admin mengatur dan menetapkan jadwal pada setiap pintu. Hal tersebut akan memudahkan jika sistem penguncian ini dipasang pada ruangan umum seperti ruang kelas atau gedung perkuliahan yang mempunyai pintu yang harus dibuka dan ditutup secara periodik.   1. Pengaturan Hak Akses   Admin juga dapat mengatur level akses dari setiap pengguna yang terdaftar sehingga hak akses dari setiap pengguna dapat disesuaikan dengan kondisi dan kebutuhan yang ada.   1. *Unlock* Cepat   Di setiap pintu yang telah terpasang perangkat penguncian akan ditandai dengan QR-*code*. Setiap pengguna (admin, pengguna, dan pengunjung) dapat memindai QR-*code* tersebut untuk membuka pintu secara cepat dan aman.   1. Keamanan   Keamanan menjadi fokus utama dalam mengerjakan proyek ini, setiap pengguna memiliki *username* dan *password* serta email sebagai identitas pengguna. Pengguna akan diminta melakukan *login* pada saat pertama kali meng-*install* aplikasi serta memasukkan kode autentikasi yang dikirim melalui email (autentikasi 2 arah). Setiap aktivitas yang dilakukan oleh pengguna akan tercatat di *database* sebagai *log* aktivitas. |

Terdapat beberapa tahapan verifikasi produk untuk menguji keandalan dari fitur sistem keamanan kunci pintu gedung berbasis *internet of things*. Verifikasi produk mencakup pengujian subsistem komunikasi dua arah dan perangkat pengunci yang mendukung sistem keamanan kunci gedung berbasis IoT, pengujian *database* dan *server*, serta sistem keamanan kunci pintu gedung dengan kontrol akses, dan subsistem perangkat *mobile* sebagai piranti akses masuk pintu gedung dan *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh.

1. **Pengujian Subsistem Komunikasi Data Dua Arah dan Perangkat Penguncian yang Mendukung Sistem Keamanan Kunci Pintu Gedung Berbasis IoT**

Pengujian ini adalah pengujian untuk memastikan bahwa subsistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT bekerja dengan baik dan sesuai dengan spesifikasi. Tujuan dari pengujian ini adalah untuk memastikan bahwa sistem keamanan kunci pintu gedung dapat berfungsi dengan benar dan memberikan akses yang sesuai bagi pengguna yang terautorisasi.

1. **Pengujian Subsistem Komunikasi Data Dua Arah**

Pengujian ini meliputi uji coba untuk memastikan bahwa sistem dapat menerima dan mengirimkan data dengan benar baik melalui komunikasi bluetooth maupun koneksi internet. Ini termasuk memastikan bahwa komunikasi antara perangkat penguncian dan *server* bekerja dengan baik dan bahwa informasi akses yang diperlukan dapat diterima dan diteruskan oleh perangkat penguncian.

*Tools* yang dapat digunakan untuk memastikan bahwa sistem dapat menerima dan mengirimkan data dengan benar melalui jaringan IoT meliputi:

* *Serial Monitor*: Perangkat lunak yang digunakan untuk menampilkan data menggunakan komunikasi serial. Data yang ditampilkan merupakan data hasil dari proses pengujian seperti status koneksi, data yang diterima dari server dan waktu yang dibutuhkan selama proses pengujian tersebut. Data tersebut kemudian dianalisa untuk menyimpulkan hasil dari pengujian yang telah dilakukan.
* *Bluetooth* *Terminal*: Perangkat lunak yang digunakan untuk berkomunikasi dengan perangkat kunci pintu dengan menggunakan bluetooth. Dengan menggunakan bluetooth terminal maka proses pengujian dilakukan dengan mengirimkan data dan menerima data sehingga diperoleh status pengiriman serta waktu yang diperlukan.

1. **Pengujian Perangkat Penguncian**

Pengujian ini meliputi uji coba untuk memastikan bahwa perangkat dapat membuka dan mengunci pintu dengan benar dan bahwa perangkat memiliki kemampuan untuk memblokir akses jika informasi akses tidak sesuai. Ini juga memastikan bahwa perangkat dapat mempertahankan informasi akses yang diterima dan memperbarui informasi akses jika diperlukan.

*Tools* yang dapat digunakan untuk memastikan bahwa perangkat dapat membuka dan mengunci pintu dengan benar dan memiliki kemampuan untuk memblokir akses jika informasi akses tidak sesuai meliputi:

* + *Test Cases*: Membuat dan menjalankan skenario uji untuk memastikan bahwa perangkat dapat membuka dan mengunci pintu dengan benar dan memiliki kemampuan untuk memblokir akses jika informasi akses tidak sesuai.
  + *Serial* *Monitor:* melakukan pengujian untuk mengukur keandalan sistem pernagkat penguncian seperti mengukur waktu yang diperlukan untuk memproses suatu perintah penguncian.

Hasil dari pengujian ini harus memastikan bahwa sistem keamanan kunci pintu gedung berbasis IoT bekerja dengan benar dan memenuhi spesifikasi yang ditentukan. Jika hasilnya positif, maka sistem dapat digunakan untuk meningkatkan keamanan dan efisiensi akses pada gedung. Namun, jika hasilnya negatif, maka perlu dilakukan perbaikan untuk memastikan bahwa sistem bekerja dengan benar.

1. **Pengujian Subsistem *Database* dan *Serve*r serta Sistem Keamanan Kunci Pintu Gedung dengan Kontrol Akses**

Pengujian pada subsistem ini dilakukan untuk memastikan bahwa subsistem *database* dan *server*, serta sistem keamanan kunci pintu gedung dengan kontrol akses bekerja dengan baik dan sesuai dengan spesifikasi. Tujuan dari pengujian ini adalah untuk memastikan bahwa sistem keamanan kunci pintu gedung dapat memberikan akses yang sesuai bagi pengguna yang terautorisasi dan bahwa informasi akses yang diperlukan dapat diterima, disimpan, dan diproses dengan benar.

* 1. **Pengujian Subsistem *Database* dan *Server***

Pengujian ini meliputi uji coba untuk memastikan bahwa informasi akses dapat disimpan dan diteruskan dengan benar melalui *server* dan *database*. Ini termasuk memastikan bahwa informasi akses yang diterima dapat diproses dan disimpan dengan benar dalam *database*, serta bahwa informasi akses dapat diteruskan dengan benar ke perangkat penguncian yang terkait.

*Tools* yang dapat digunakan untuk memastikan bahwa informasi akses dapat disimpan dan diteruskan dengan benar melalui *server* dan *database* meliputi:

* *Postman*: Perangkat lunak yang digunakan untk melakukan pengujian terhadap fungsionalitas dan performa API. Dengan menggunakan *postman* kinerja *server* dan *database* dalam memproses data berdaparkan permintaan *client* dapat diuji baik dari segi fungsionalitas dan performanya.
* *Jmeter*: perangkat lunak yang digunakan untuk melakukan pengujian performa dari sebuah layanan website atau API dengan mensimulasikan beban permintaan pengguna secara bersamaan. Dengan adanya pengujian beban maka dapat diperoleh informasi mengenai performa sistem yang telah dibuat.
  1. **Pengujian sistem keamanan kunci pintu gedung dengan kontrol akses** Pengujian ini meliputi uji coba untuk memastikan bahwa sistem dapat membuka dan mengunci pintu dengan benar, serta memblokir akses jika informasi akses tidak sesuai. Ini juga memastikan bahwa sistem dapat mempertahankan informasi akses yang diterima dan memperbarui informasi akses jika diperlukan.

*Tools* yang dapat digunakan untuk memastikan bahwa sistem dapat membuka dan mengunci pintu dengan benar dan memblokir akses jika informasi akses tidak sesuai meliputi:

* *Postman*: Perangkat lunak yang digunakan untuk melakukan pengujian API, dengan menggunakan postman pengujian dilakukan dengan melakukan permintaan ke API dengan berbagai kondisi data seperti pengguna yang memiliki akses dan tidak memiliki akses.
* Aplikasi Kunci Pintu*:* Pengujian dilakukan dengan menggunakan aplikasi kunci pintu yang telah dibuat dengan memeriksa beberapa fitur seperti kode QR untuk mendapatkan kunci akses pintu.

Hasil dari pengujian ini harus memastikan bahwa sistem keamanan kunci pintu gedung dengan kontrol akses bekerja dengan benar dan memenuhi spesifikasi yang ditentukan. Jika hasilnya positif, maka sistem dapat digunakan untuk meningkatkan keamanan dan efisiensi akses pada gedung. Namun, jika hasilnya negatif, maka perlu dilakukan perbaikan untuk memastikan bahwa sistem bekerja dengan benar.

1. **Pengujian Subsistem** **Perangkat *Mobile* sebagai PirantiAkses Masuk Pintu Gedung dan *Website* untuk Mendukung Sistem *Monitoring* dan *Controlling* Jarak Jauh**

Pengujian ini adalah adalah pengujian untuk memastikan bahwa subsistem aplikasi *mobile* dan *website* bekerja dengan baik dan sesuai dengan spesifikasi sebagai piranti akses masuk pintu gedung dan dukungan sistem *monitoring* dan *controlling* jarak jauh. Tujuan dari pengujian ini adalah untuk memastikan bahwa perangkat *mobile* dapat digunakan dengan mudah sebagai alat akses masuk pintu gedung dan bahwa *website* dapat memberikan *monitoring* dan *controlling* jarak jauh yang efisien.

* + 1. **Pengujian Subsistem Aplikasi *Mobile***

Pengujian ini meliputi uji coba untuk memastikan bahwa aplikasi *mobile* dapat terhubung dan berkomunikasi dengan sistem keamanan kunci pintu gedung dengan benar. Ini termasuk memastikan bahwa perangkat *mobile* dapat mengirimkan informasi akses yang dibutuhkan untuk membuka pintu dan memastikan bahwa perangkat *mobile* dapat menerima informasi dari sistem keamanan kunci pintu gedung.

Untuk memastikan bahwa perangkat *mobile* dapat terhubung dan berkomunikasi dengan sistem keamanan kunci pintu gedung dengan benar, beberapa *tools* yang dapat digunakan antara lain:

* *Android Profiler*: Merupakan sebuah fitur pada pengembangan aplikasi android yang digunakan untuk mengukur performa aplikasi saat sedang dijalankan seperti mengukur penggunaan ruang penyimpanan, waktu respon dan lain sebagainya.
* *Test Cases*: Menggunakan skenario pengujian untku memeriksa kinerja dari masing-masing fitur pada berbagai jenis smartphone.
  + 1. **Pengujian *website***

Pengujian ini meliputi uji coba untuk memastikan bahwa *website* dapat menampilkan informasi yang dibutuhkan untuk *monitoring* dan *controlling* sistem keamanan kunci pintu gedung. Ini termasuk memastikan bahwa *website* dapat memberikan informasi akses dan status pintu gedung dan bahwa *website* dapat digunakan untuk memperbarui informasi akses dan memblokir akses jika diperlukan.

Untuk memastikan bahwa *website* dapat berfungsi sebagaimana mestinya dalam memantau dan mengontrol sistem keamanan kunci pintu gedung, beberapa alat pengujian yang digunakan dapat meliputi:

* Jmeter: Perangkat lunak yang digunakan untk melakukan pengujian performa dari website dengan mengukur waktu respon serta mensimulasikan beban pengguna yang banyak.
* *Browser*: Perangkat lunak yang digunakan untuk menampilkan konten dari sebuah *website*. Dengan menggunakan *browser* pengujian dilakukan untuk memastikan semua fitur dapat bekerja dengan baik pada berbagai jenis *browser*.
* *Test Cases*: Menggunakan skenario pengujian untuk memeriksa kinerja dari masing-masing fitur yang disediakan oleh website dengan berbagai kondisi yang ada.
* *Mobile Simulator*: Sebuah perangkat lunak yang digunakan untku menampilkan konten website pada berbagai ukuran layar, dengan menggunakan mobile simulator pengujian dilakukan untuk memastikan bahwa tampilakn website bisa menyesuaikan dengan berbagai macam ukuran layar.

Hasil dari pengujian ini harus memastikan bahwa perangkat *mobile* dan *website* bekerja dengan benar dan memenuhi spesifikasi yang ditentukan. Jika hasilnya positif, maka perangkat *mobile* dan *website* dapat digunakan untuk meningkatkan efisiensi dan keamanan akses pada gedung. Namun, jika hasilnya negatif, maka perlu dilakukan perbaikan untuk memastikan bahwa perangkat *mobile* dan *website* bekerja dengan benar.

## **Biaya dan Jadwal**

1. **Analisis Biaya**

Analisis biaya yang dibutuhkan dalam rancang bangun sistem keamanan kunci pintu gedung berbasis IoT dapat dilihat pada Tabel 2.2 di bawah ini.

Tabel 2.2 Perkiraan Biaya

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Pengeluaran** | **Jumlah** | **Harga (Rp)** | **Total (Rp)** |
| 1 | Mikrokontroler ESP32 | 2 buah | 70.000 | 140.000 |
| 2 | Sensor magnetik | 2 buah | 10.000 | 20.000 |
| 3 | Kabel | 5 meter | 2.500 | 12.500 |
| 4 | Cetak PCB | 4 buah | 25.000 | 100.000 |
| 5 | Baut, mur, *spacer* | 2 buah | 15.000 | 30.000 |
| 6 | Adaptor 12 Volt | 2 buah | 20.000 | 40.000 |
| 7 | Tombol | 2 buah | 3.000 | 6.000 |
| 8 | *Server* | 5 buah | 120.000 | 600.000 |
| 9 | Solenoida | 2 buah | 40.000 | 80.000 |
| 10 | Kusen Pintu | 2 buah | 150.000 | 300.000 |
| Jumlah Total | | |  | **1.328.500** |

1. **Jadwal**

Proyek rancang bangun sistem keamanan kunci pintu gedung berbasis IoT dirancang untuk rentang 6 bulan, dimulai pada Maret 2023 – Agustus 2023. *Time* *table* proyek ini dapat dilihat pada Tabel 2.3.

**Tabel 2.3** Jadwal dan Waktu Pengembangan

|  |  |  |  |
| --- | --- | --- | --- |
| **Fase** | ***Deliverables*** | **Jadwal** | **Kebutuhan Sumber Daya** |
| Konsep Produk | Dokumen B100  Proposal | Maret 2023 | Literatur |
| Analisis | Dokumen B200  Spesifikasi Fungsional | April 2023 | 1. Spek standar 2. *Engineer* |
| Desain | Dokumen B300 Skematik Rangkaian Rancangan | April 2023 | 1. *Dvlp. Tools* 2. Penguasaan teknologi pendukung 3. Literatur 4. *Engineer* |
| Implementasi (Pedoman standar perencanaan) | Dokumen B400  Lab Redesain | Mei - Juni 2023 | 1. *Dvlp*. *Tools* 2. *Software Cadsoft Eagle* 3. *Software Android Studio* 4. *Engineer* 5. Komponen-komponen *hardware* |
| Pengujian subsistem | Dokumen B500  *Error Report*, redesain skematik, ralat kode program | Juli 2023 | 1. *Dvlp*. *Tools* 2. *Software Cadsoft Eagle* 3. *Engineer* |
| Laporan Akhir | Dokumen Laporan | Agustus 2023 | 1. Dvlp. Tools 2. Mekanisme Pelaporan |

1. PENUTUP

Dokumen B200 memaparkan fungsi, spesifikasi, dan fitur dari produksistem keamanan kunci pintu gedung berbasis *internet of things*. Proses verifikasi dari fungsionalitas sistem keamanan kunci pintu gedung berbasis *internet of things* meliputi pengujian pada subsistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT, pengujian subsistem *database* dan *serve*r serta sistem keamanan kunci pintu gedung dengan *Access Control,* serta subsistem perangkat *mobile* sebagai pirantiakses masuk pintu gedung dan *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh. Hasil perancangan spesifikasi pada dokumen B200 akan dijadikan acuan untuk pembuatan desain produk sistem keamanan kunci pintu gedung berbasis *internet of things*, acuan pelaksanaan proyek, dan acuan pengujian fitur produk.