BAB II
TINJAUAN PUSTAKA

2.1. LANDASAN TEORI

Landasan teori merupakan penjelasan berbagai konsep dasar dan teori-teori yang berkaitan dalam pembangunan Broker Aedes

2.1.1 IoT

Internet of things merupakan sebuah konsep di mana suatu benda atau objek ditanamkan teknologi-teknologi seperti sensor dan software dengan tujuan untuk berkomunikasi, mengendalikan, menghubungkan, dan bertukar data melalui perangkat lain selama masih terhubung ke internet. IoT memiliki hubungan yang erat dengan istilah machine-to-machine atau M2M. Seluruh alat yang memiliki kemampuan komunikasi M2M ini sering disebut dengan perangkat cerdas atau smart devices. Perangkat cerdas ini diharapkan dapat membantu kerja manusia dalam menyelesaikan berbagai urusan atau tugas yang ada. Dengan adanya teknologi Internet of Things ini proses kerja sebuah sistem dapat dilakukan semangkin luas, jarak jangkauannya juga semangkin luas, proses pengolahan data dan analisis data terhadap sebuah sistem juga semangkin bagus. Teknologi IoT ini benar-benar mendukung kerja sistem sebagai suatu kesatuan meliputi komponen/elemen dalam hal memudahkan proses aliran informasi data. Sistem pada penelitian ini mengabungkan tiga bagian penting, yaitu mekanik, hardware (elektronik) dan algoritma kontrol, dimana ketiga bagian tersebut saling berinteraksi dan tidak dapat dipisahkan dalam satu kesatuan sistem. [22,23]

2.2.2 MQTT

Protokol MQTT (Message Queuing Telemetry Transport) adalah protokol yang berjalan pada diatas stack TCP/IP dan mempunyai ukuran paket data dengan low overhead yang kecil (minimum 2 bytes) sehingga berefek pada konsumsi catu daya yang juga cukup kecil.MQTT adalah protokol messaging yang dibentuk dengan TCP/IP berdasarkan model messaging publish-subscribe. Publisher mengirim pesan, subscriber menerima pesan yang mereka sukai, dan

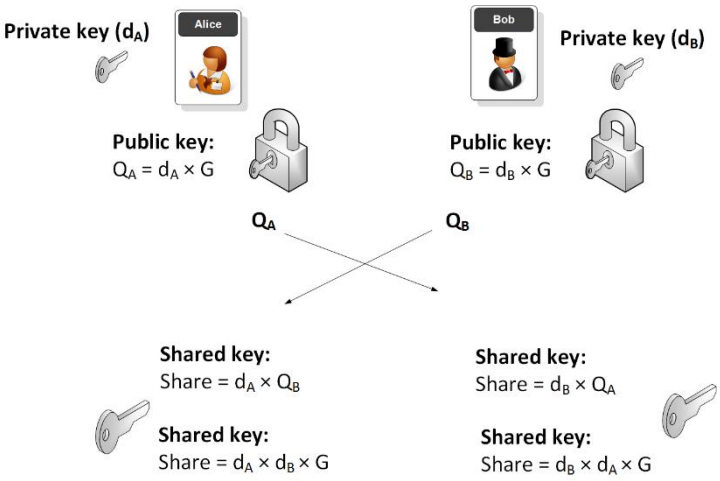
broker akan menyampaikan pesan dari pengirim ke penerima. Publisher dan subscriber adalah klien MQTT yang hanya berkomunikasi dengan broker MQTT. Klien MQTT dapat berupa perangkat atau aplikasi apapun (dari mikro kontroler seperti Arduino sampai dengan aplikasi penuh yang di host di Cloud) yang menjalankan MQTT library dan mengkoneksikan ke broker MQTT melalui sebuah jaringan. Broker MQTT mengelola penerimaan pesan dari publisher dan pengiriman pesan ke subscriber (dan juga mengelola daftar topik yang disukai subscriber).MQTT adalah protokol terkemuka untuk menghubungkan perangkat IoT dan menggeser HTTP, andalan di dunia internet di tahun 2017. Terlebih lagi, MQTT telah dipilih protokol messaging untuk platform IoT seperti Amazon, Microsoft, IBM, dan produk open-source dan broker komersial lainnya.[15]

2.2.3 Broker

Broker pada MQTT berfungsi untuk menghandle data publish dan subscribe dari berbagai device, bisa diibaratkan sebagai server yang memiliki alamat IP khusus. Beberapa contoh dari Broker yang ada seperti Mosquitto, HiveMQ dan Mosca ataupun Aedes.Publish merupakan cara suatu device untuk mengirimkan datanya ke subscribers. Biasanya pada publisher ini adalah sebuah device yang terhubung dengan sensor tertentu. Subscribe merupakan cara suatu device untuk menerima berbagai macam data dari publisher. Subscriber dapat berupa aplikasi monitoring sensor dan sebagainya, subscriber ini yang nantinya akan meminta data dari publisher.Topic seperti halnya pengelompokan data disuatu kategori tertentu. Pada sistem kerja MQTT protokol ini, topic bersifat wajib hukumnya. Pada setiap transaksi data antara Publisher dan Subscriber harus memiliki suatu topic tertentu. [12]

2.2.4 Elliptic Curve Diffie-Hielman

Algoritma lliptic Curve Diffie-Hellman (ECDH) merupakan sebuah protokol perjanjian kunci anonim yang memungkinkan dua pihak, A dan B, untuk membangun kunci rahasia bersama (share secret key) melalui saluran yang tidak aman, di mana masing-masing pasangan memiliki kunci public dan kunci private berbasis elliptic curve. Share secret tersebut nantinya dapat digunakan sebagai kunci untuk kriptografi kunci simetris



Gambar 2.4 Elliptic Curve Diffie Hielman

Untuk generasi kunci rahasia bersama antara A dan B menggunakan ECDH, keduanya harus setuju atas parameter domain EC. Keduanya akhirnya memiliki sepasang kunci yang terdiri dari kunci d privat (integer dipilih secara acak yang bernilai lebih kecil dari n , dimana n adalah urutan kurva) dan satu lagi adalah kunci publik Q = d * G (G adalah titik pembangkit) . Biarkan (dA , QA) menjadi pasangan kunci publik-privat A dan (dB , QB) menjadi kunci privat - publik B.

1. A Menghitung KA = (XA, YA) = dA * QB

2. B Menghitung KB = (XB, YB) = dB * QA

3. Sejak dA * QB = dAdB G = G = dBdA dB * QA

Oleh karena KA = KB dan karenanya XA = XB. (Dimana G adalah titik pembangkit). Oleh karena itu share secret adalah KA.Karena hampir mustahil untuk menemukan kunci pribadi dA atau dB dari KA kunci publik [13]

2.2.5 Advanced Encryption Standard (AES)

AES merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES menggunakan proses yang berulang yang disebut dengan ronde. Proses di dalam AES merupakan transformasi terhadap state. Sebuah teks asli dalam blok (128 bit) terlebih dahulu diorganisir sebagai state. Enkripsi AES adalah transformasi terhadap state secara berulang dalam beberapa ronde. State yang menjadi keluara ronde k menjadi masukan untuk ronde ke-k +1.

AES merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES menggunakan proses yang berulang yang disebut dengan ronde. Proses di dalam AES merupakan transformasi terhadap state. Sebuah teks asli dalam blok (128 bit) terlebih dahulu diorganisir sebagai state. Enkripsi AES adalah transformasi terhadap state secara berulang dalam beberapa ronde. State yang menjadi keluara ronde k menjadi masukan untuk ronde ke-k +1. Pada Proses enkripsi awalnya teks asli dibentuk sebagai sebuah state. Kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini disebut AddRoundKey). 120 | Aditia Rahmat Tulloh, et al. Volume 2, No.2, Tahun 2016 Setelah itu, ronde ke-1 sampai dengan ronde ke-(Nr-1) dengan Nr adalah jumlah ronde. AES menggunakan 4 jenis transformasi yaitu:

1. SubBytes, sebagai transformasi subtutusi.

2. ShiftRows, sebagai transformasi permutasi.

3. MixColumns, sebagai transformasi pengacakan.

4. AddRoundKey, sebagai transformasi penambahan kunci.

Pada ronde terakhir, yaitu ronde ke-Nr dilakukan transformsi serupa dengan ronde lain namun tanpa transfomasi serupa dengan ronde lain namun tanpa transformasi MixColumns. [14]

2.2.6 UML

UML adalah salah satu tool/model untuk merancang pengembangan software yang berbasis object-oriented. UML sendiri juga memberikan standar penulisan sebuah sistem blueprint, yang meliputi konsep proses bisnis, penulisan kelas-kelas dalam bahasa program yang spesifik, skema database, dan komponen yang diperlukan dalam sistem software.[16,17]

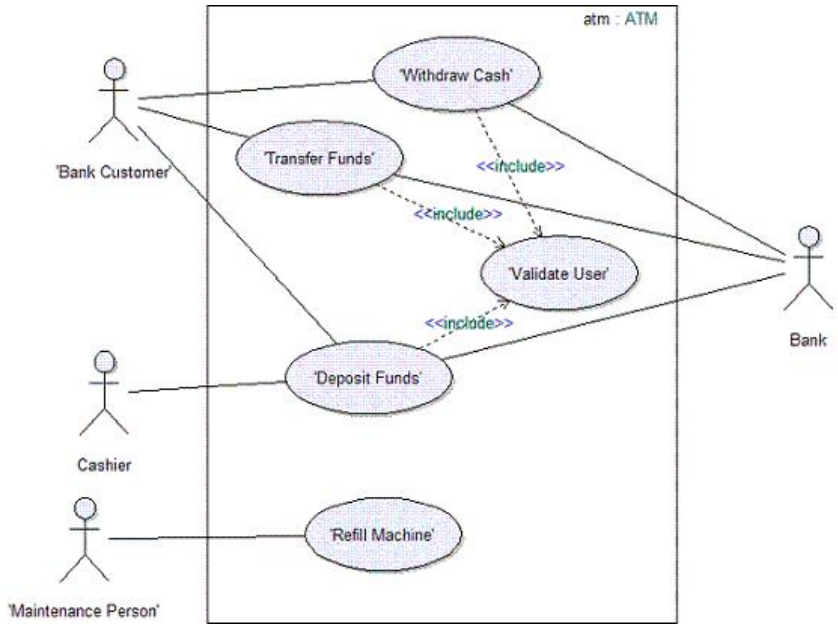
UML hanya berfungsi untuk melakukan pemodelan. Jadi penggunaan UML tidak terbatas pada metodologi tertentu, meskipun pada kenyataannya UML paling banyak digunakan pada metodologi berorientasi objek Jenis –Jenis Diagram Unified Modeling

1. Language (UML)
2. Use Case Diagram
3. Class Diagram
4. Activity Diagram
5. Sequence Diagram
6. State Diagram
7. Collaboration Diagram
8. Deployment Diagram

2.2.7 Use Case Diagram

use case diagram adalah proses penggambaran yang dilakukan untuk menunjukkan hubungan antara pengguna dengan sistem yang dirancang. Hasil representasi dari skema tersebut dibuat secara sederhana dan bertujuan untuk memudahkan *user* dalam membaca informasi yang diberikan. Use case diagram terdiri dari sebuah aktor dan interaksi yang dilakukannya, aktor tersebut dapat berupa 9 manusia, perangkat keras, sistem lain, ataupun yang berinteraksi dengan

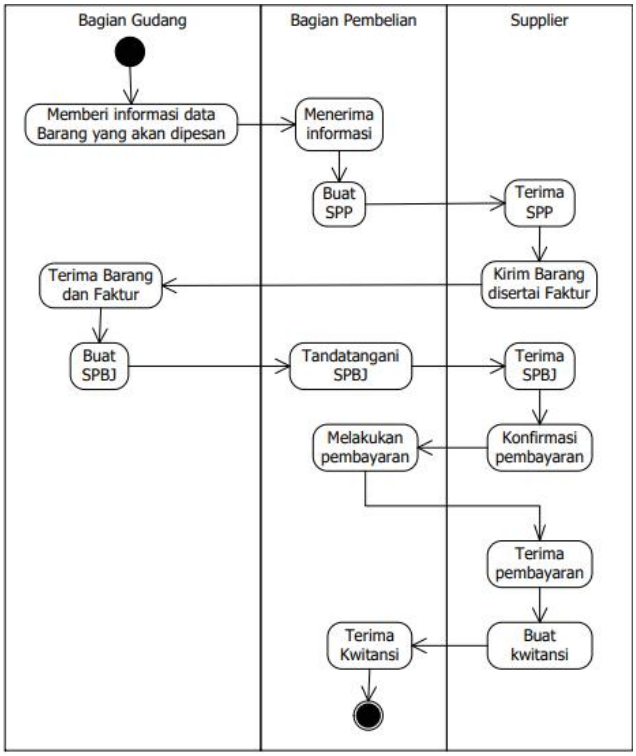
sistem. Pada aplikasi pencarian jalur terpendek antar kota menggunakan algoritma genetika, use case menjelaskan tentang hubungan antara sistem dengan aktor. Hubungan ini dapat berupa inputaktor ke sistem ataupun output ke aktor. Use case merupakan dokumen naratif yang mendeskripsikan kasuskasus atau kejadian-kejadian daripada aktor dalam menggunakan sistem untuk menyelesaikan sebuah proses.[18]



Gambar 2.5 Contoh Use Case Diagram

2.2.8 Activity Diagram

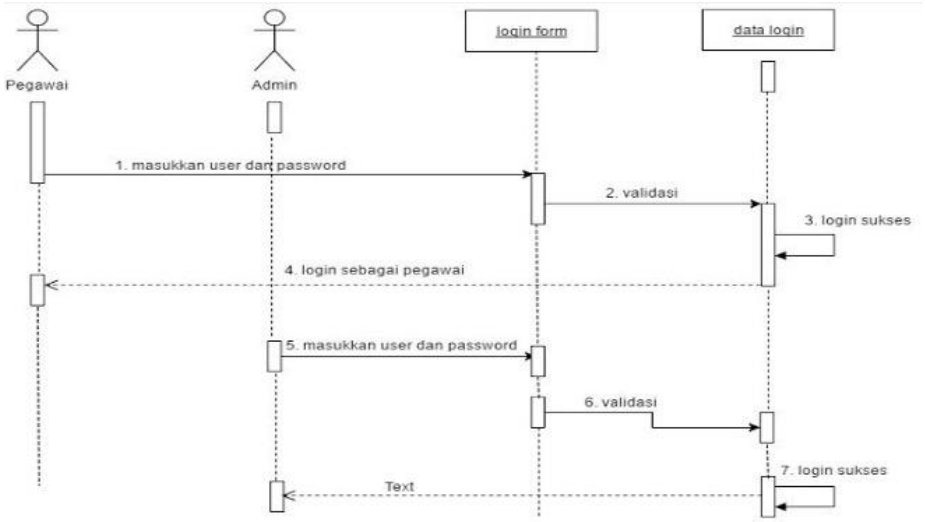
Activity Diagram merupakan rancangan aliran aktivitas atau aliran kerja dalam sebuah sistem yang akan dijalankan. Activity Diagram juga digunakan untuk mendefinisikan atau mengelompokan aluran tampilan dari sistem tersebut. Activity Diagram memiliki komponen dengan bentuk tertentu yang dihubungkan dengan tanda panah. Panah tersebut mengarah ke-urutan aktivitas yang terjadi dari awal hingga akhir. Activity diagram juga dapat menggambarkan proses pararel yang mungkin terjadi pada beberapa eksekusi. [18]



Gambar 2.6 Contoh Activity Diagram

2.2.9 Sequence Diagram

Sequence diagram menggambarkan interaksi antar objek di dalam dan di sekitar sistem (termasuk pengguna, display, dan sebagainya) berupa message yang digambarkan terhadap waktu. Sequence diagram terdiri atar dimensi vertikal (waktu) dan dimensi horizontal (objek-objek yang terkait).Sequence diagram digunakan untuk menggambarkan interaksi antar objek di dalam dan di sekitar sistem yang berupa message yang digambarkan terhadap waktu. Sequence diagram terdiri antara dimensi vertical (waktu) dan dimensi horizontal (objek-objek yang terkait)[18]



Gambar 2.7 Contoh Sequence Diagram

2.2.10 Node Js

Node.js framework atau Node merupakan perangkat lunak berbasis JavaScript yang bersifat *open-source,* dapat dijalankan dalam lingkungan lintas platform untuk mengeksekusi kode JavaScript di luar browser. Secara tradisional, browser menyediakan lingkungan runtime untuk kode JS. Node Js dapat disebut juga runtime environment. Aplikasi ditulis dalam campuran Bahsa C++ dan juga Jvascript, mempunyai model event driver (basis event) dan asynchronous I/O. Node Js diekskusi sebagai aplikasi server dengan dukungan V8 Enginer buatan Google dan beberapa modul bawaan yang terintegrasi seperti modul http, modul file system, modul security dan beberapa modul penting lainya [19]

2.2.11 Raspberry Pi

Raspberry Pi, sering disingkat dengan nama Raspi, adalah komputer papan tunggal (*single-board circuit*; SBC) yang seukuran dengan kartu kredit yang dapat digunakan untuk menjalankan program perkantoran, permainan komputer, dan sebagai pemutar media hingga video beresolusi tinggi. Raspberry Pi dikembangkan oleh yayasan nirlaba, Rasberry Pi Foundation, yang digawangi sejumlah pengembang dan ahli komputer dari Universitas Cambridge, Inggris.

Ide dibalik Raspberry Pi diawali dari keinginan untuk mencetak pemrogram generasi baru. Seperti disebutkan dalam situs resmi Raspberry Pi Foundation, waktu itu Eben Upton, Rob Mullins, Jack Lang, dan Alan Mycroft, dari Laboratorium Komputer Universitas Cambridge memiliki kekhawatiran melihat kian turunnya keahlian dan jumlah siswa yang hendak belajar ilmu komputer. Mereka lantas mendirikan yayasan Raspberry Pi bersama dengan Pete Lomas dan David Braben pada 2009. Tiga tahun kemudian, Raspberry Pi Model B memasuki produksi massal. Dalam peluncuran pertamanya pada akhir Febuari 2012 dalam beberapa jam saja sudah terjual 100.000 unit. Pada bulan Februari 2016, Raspberry Pi Foundation mengumumkan bahwa mereka telah menjual 8 juta perangkat Raspi, sehingga menjadikannya sebagai perangkat paling laris di Inggris. [20]

2.2.12 Arduino UNO

Arduino Uno adalah salah satu jenis papan mikrokontroler berbasis ATmega328, dan Uno adalah istilah bahasa Italia yang artinya satu. Arduino Uno dinamai untuk menandai peluncuran papan mikrokontroler yang akan datang yaitu Arduino Uno Board 1.0. Papan ini mencakup pin-14 I / O digital, colokan listrik, i / ps-6 analog, resonator keramik-A16 MHz, koneksi USB, tombol RST, dan header ICSP. Semua ini dapat mendukung mikrokontroler untuk operasi lebih lanjut dengan menghubungkan papan ini ke komputer. Catu daya papan ini dapat dilakukan dengan bantuan adaptor AC ke DC, kabel USB, atau baterai. Artikel ini membahas tentang apa itu mikrokontroler Arduino Uno, konfigurasi pin, spesifikasi atau fitur Arduino Uno, dan aplikasi.[21]