

BAB II

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian tentang *Internet of Things* khususnya dibidang *smart home* sudah banyak dilakukan dan sudah banyak diterapkan diberbagai bidang, baik dalam bidang kontrol lampu, pendeteksi polusi gas rumah, alarm, dan lain sebagainya. Dalam penelitian yang sudah dilakukan sebelumnya menunjukkan bahwa *Internet of Things* khususnya *smart home* sangat dibutuhkan untuk mempermudah pemilik rumah dalam memantau keadaan rumah. Berikut merupakan beberapa penelitian terdahulu:

Berdasarkan penelitian yang dilakukan oleh Sinar Monika, Abdul Rakhman, dan Lindawati pada tahun 2017, mengenai pengaman rumah dengan sistem *face recognition* secara *real time* menggunakan metode *Principal Component Analysis (PCA)*. Penelitian ini bertujuan untuk membantu pemilik rumah untuk mengamankan aset-aset yang terdapat di rumah dengan membuat suatu sistem pengaman rumah yang menerapkan sistem *face recognition* dengan menggunakan metode *PCA*. Perancangan sistem menggunakan *software visual studio 2015* yang menghasilkan tingkat akurasi sebesar 88% dalam melakukan pencocokan wajah pemilik rumah [8].

Penelitian yang dilakukan oleh Sehman pada tahun 2015 mengenai penerapan *face recognition* dengan metode *Eigenface* pada *intelligent car security* yang menceritakan mengenai kejadian pencurian terhadap kendaraan, dikarenakan proteksi alarm yang terdapat di mobil dapat dengan mudahnya dijebol dan dirusak. Dengan adanya permasalahan tersebut, peneliti membuat suatu inovasi terbaru untuk kendaraan. Hasil penelitian ini membuat rancangan alat yang dapat meminimalisir tindak kejahatan pencurian khususnya pada kendaraan. Dengan menerapkan *face recognition* yang dikode dan disimpan

didatabase dengan bantuan mikrokontroller AVR yang bekerja layaknya mikrokontroller nodemcu esp8266, dimana implementasi alat ini diletakkan di pintu dekat kemudi [7].

Penelitian yang dilakukan oleh Shubhang Khattar, Annisa Sachdeva, Rishi Kumar, dan Richa Gupta pada tahun 2019 mengenai *smart home with virtual assistant using Raspberry Pi* yang dilatari oleh permasalahan tindak kejahatan pencurian dan perampokan yang terjadi di negara india terhadap rumah marak terjadi. Semakin majunya teknologi, *developer* berlomba-lomba dalam membuat *virtual assistant* seperti yang dilakukan Google dengan nama *Alexa*, Apple dengan nama *Siri*, dan Windows dengan produknya yaitu *Cortana*. Dari hal tersebut muncul kegiatan *monitoring* yang dapat dibantu dengan menerapkan *virtual assistant* yang bernama *Ollivia*, dengan menggunakan *voice recognition* dan *face recognition*. Penelitian ini menggunakan *single board computer* Raspberry Pi yang di integrasikan dengan internet sehingga dapat meminimalisir apabila terjadi tindak kejahatan [9].

Penelitian serupa juga dilakukan oleh Muhammad Izzudin Mahali pada tahun 2016 mengenai *smart door locks based on Internet of Things concept with mobile backend as a service* yang bertujuan menciptakan teknologi kunci pintu secara digital dengan memanfaatkan *cloud computing* sebagai media penyimpanan data dengan menerapkan konsep *Internet of Things* yang dikendalikan melalui sistem website. Pengembangan sistem ini menghasilkan sistem yang dapat terhubung dengan mikrokontroller. Sistem dapat melakukan penguncian dan pembukaan pintu melalui aplikasi sistem website [10].

Penelitian tersebut juga dilakukan oleh Rijal Permana, Unang Surya, dan Rumani M pada tahun 2017 mengenai perancangan sistem keamanan dan kontrol *smart home* berbasis *Internet of Things*. Tujuan penelitian ini yaitu melakukan kegiatan *monitoring* dan juga mengontrol keadaan rumah. perancangan sistem ini dapat dikendalikan jarak jauh dengan menerapkan *Internet of Things* sebagai narahubung sistem *website* dengan mikrokontroller.

Hasil dari penelitian ini dapat mengontrol kelembapan, suhu, dan kadar karbon dioksida, serta sistem ini dapat melakukan keamanan rumah dengan memasang beberapa sensor gerak yang dapat memicu kamera menyala untuk memantau aktifitas yang terjadi didalam maupun sekitar rumah. sensor yang digunakan dalam penelitian ini diantaranya yaitu : sensor suhu DHT22, sensor gerak PIR, sensor gas MQ-135, dan kamera dengan menggunakan mikrokontroler esp8266 dan Raspberry Pi [11].

Penelitian *face recognition* juga dilakukan oleh Luisan William Alexander, Steven Ray Sentinuwo, dan Alwin Melkie Sambul pada tahun 2017 mengenai implementasi algoritma pengenalan wajah untuk mendeteksi *visual hacking*. Penelitian ini bertujuan untuk mendeteksi adanya *visual hacking* yang terjadi di lingkungan kerja. *Visual hacking* sangat merugikan karena orang lain dapat dengan mudah melihat maupun akses komputer seseorang secara langsung ketika komputer dioperasikan dan ditinggal oleh pemilik komputer. Penelitian ini membuat suatu inovasi terbaru dengan mengimplementasikan sistem pengenalan wajah. Sistem dirancang untuk mengurangi tindakan *visual hacking* berupa menguntit atau melihat secara langsung terhadap layar monitor. Hasil penelitian ini adalah dapat mendeteksi oknum – oknum yang melakukan tindakan *visual hacking* melalui implementasi algoritma pengenalan wajah. Outputnya ketika sistem mendeteksi wajah yang bukan milik komputer maka komputer akan mengunci layar, dan apabila pemilik sedang melakukan aktivitas dengan komputernya kemudian terdapat penyusup maka komputer akan memberitahukan kepada pemilik berupa icon terkunci [12].

Dari penjelasan diatas, ringkasan penelitian yang relevan ditunjukkan pada Tabel 2.1 dibawah ini:

Tabel 2.1 Penelitian Terdahulu

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
1	Pengaman Rumah Dengan Sistem <i>Face Recognition</i> Secara <i>Real Time</i> Menggunakan Metode <i>Principal Component Analysis</i> [8]	2017	<i>Principal Component Analysis (PCA)</i> .	Rumah merupakan tempat aset-aset disimpan. Masalah keamanan rumah menjadi suatu momok yang diinginkan pemilik rumah dengan harapan terhindar dari tindakan kriminal.	Menghasilkan sistem yang dapat mendeteksi wajah pemilik rumah dengan tingkat akurasi yang tinggi.	Perbedaan penelitian ini dengan milik penulis adalah metode yang digunakan dan alat yang digunakan. Dalam penelitian ini menggunakan metode <i>Principal Component Analysis (PCA)</i> dan menggunakan <i>software Visual Studio 2015</i> dalam melakukan pemantauan keadaan rumah, sedangkan penulis menggunakan metode <i>Eigenface</i> dan alat yang digunakan <i>Raspberry Pi</i> sehingga output dari sistem melalui sistem <i>website</i> .

Tabel 2.1 Penelitian Terdahulu (lanjutan)

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
2	Penerapan <i>Face recognition</i> dengan Metode <i>Eigenface</i> Pada <i>Intelligent Car Security</i> [7]	2015	<i>Eigenface</i>	Tindakan kriminal meningkat terutama dari pencurian. Mobil salah satu target unit yang selalu diincar. Keamanan mobil masih berupa alarm pada umumnya.	Menghasilkan sistem yang dapat mendeteksi wajah pemilik kendaraan dan dapat memicu bunyi alarm apabila citra wajah berbeda, serta otomatisasi penguncian pintu mobil	Perbedaan penelitian ini dengan milik penulis adalah alat dan objek pebelitiannya. penelitian ini dilakukan untuk kendaraan mobil dan menggunakan <i>microcontroller</i> AVR serta menggunakan <i>code vision</i> , sedangkan milik penulis dilakukan untuk rumah dan menggunakan Raspberry Pi serta terintegrasikan dengan sistem <i>website</i> .

Tabel 2.1 Penelitian Terdahulu (lanjutan)

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
3	<i>Smart home With Virtual Assistant Using Raspberry Pi</i> [9]	2017	<i>Eigenface</i>	Banyaknya inovasi yang terjadi di <i>smartphone</i> seperti <i>Siri</i> , <i>Cortana</i> , dan <i>Alexa</i> . tidak adanya <i>Virtual Assistant</i> yang dapat mengontrol rumah.	Menghasilkan sebuah sistem <i>Virtual Assistant</i> dengan nama <i>OLIVIA</i> . Sistem ini dibuat untuk mengontrol rumah dan juga <i>memonitoring</i> rumah.	Perbedaan penelitian ini dengan milik penulis adalah penelitian ini dibuat dengan menggunakan <i>virtual assistant</i> sehingga dapat berinteraksi dengan orang disekitar pintu rumah, sistem menggunakan <i>push</i> notifikasi berupa pesan melalui <i>SMS</i> dan <i>Email</i> . Sedangkan milik penulis sistem <i>website</i> sebagai <i>monitoring</i> serta melakukan <i>push</i> notifikasi melalui sistem <i>website</i> yang dibuat.

Tabel 2.1 Penelitian Terdahulu (lanjutan)

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
4	<i>Smart Door Locks Based On Internet of Things Concept With Mobile Backend as a Service</i> [10]	2016	<i>Internet of Things</i>	Pengembangan sistem pengunci manual ke dalam digital.	Menghasilkan sistem yang dapat mengunci pintu atau membuka pintu secara <i>remote</i> dari jarak jauh.	Perbedaan penelitian ini dengan milik penulis adalah alat yang digunakan dan metode penelitiannya. penelitian ini dibangun dengan menggunakan mikrokontroler ESP8266 dan memanfaatkan sistem <i>website</i> , sedangkan milik penulis sistem yang dirancang akan melakukan pencocokan wajah dengan metode <i>Eigenface</i> dan sistem dapat menangkap wajah yang berbeda dengan pemilik rumah.

Tabel 2.1 Penelitian Terdahulu (lanjutan)

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
5	Perancangan Sistem Keamanan dan Kontrol <i>Smart home</i> Berbasis Internet of Things[11]	2017	<i>Internet of Things</i>	Keamanan rumah merupakan masalah utama yang dipikirkan pemilik rumah. Seringnya tindak pencurian yang menasar rumah kosong atau sedang ditinggal pemilik.	Menghasilkan sistem yang dapat memonitor dan kontrol rumah secara <i>real time</i>	Perbedaan penelitian ini dengan milik penulis adalah metode dan alat yang digunakan. penelitian ini melakukan <i>monitoring</i> dan juga mengontrol rumah dengan menggunakan mikrokontroller nodemcu esp8266 dan Arduino uno dengan memanfaatkan sistem <i>website</i> sebagai media <i>monitoring</i> . Sedangkan penulis menggunakan melakukan <i>monitoring</i> dengan memanfaatkan pengaplikasian <i>face recognition</i> dengan metode <i>Eigenface</i> dan menggunakan <i>single board computer</i> Raspberry Pi.

Tabel 2.1 Penelitian Terdahulu (lanjutan)

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
6	Implementasi Algoritma Pengenalan Wajah Untuk Mendeteksi <i>Visual Hacking</i> [12]	2017	<i>Eigenface, Viola Jones Framework</i>	Sering terjadinya <i>visual hacking</i> berupa penyusupan ketika kondisi layat monitor komputer menyala. Hal ini biasa terjadi diperkantoran. Tidak otomatis mengunci pada layar ketika adanya orang yang berbeda dalam menggunakan komputer maupun dalam memantau komputer.	Menghasilkan yang dapat melakukan penguncian terhadap layar monitor ketika terjadi Gerakan penyusupan terhadap layar monitor komputer.	Perbedaan penelitian ini dengan milik penulis adalah penerapan dan alat yang digunakan. penelitian ini dibuat untuk mendeteksi <i>visual hacking</i> terhadap komputer sehingga sistem dibuat dengan melalui <i>software</i> desktop komputer, sedangkan milik penulis untuk <i>memonitoring</i> keamanan rumah dengan menggunakan alat Raspberry Pi dan sistem <i>website</i> .

2.2 Landasan Teori

Berdasarkan permasalahan dan penelitian yang akan dilakukan, adapun landasan teori yang digunakan sebagai pedoman dan pengetahuan mengenai penelitian sistem keamanan rumah dengan menerapkan beberapa bahan dan alat yang akan digunakan, diantaranya yaitu sebagai berikut:

2.2.1 *Smart Home*

Smart home merupakan suatu perangkat yang terintegrasi dengan konsep *Internet of Things* yang memungkinkan untuk mengkoleksi data, memproses data, dan merubah data. *Smart home* memberikan beberapa kemungkinan bagi pengguna untuk mengontrol, dan menyesuaikan rumah berdasarkan keinginan pemilik[13]. *Smart home* adalah sebuah tempat tinggal atau kediaman yang menghubungkan jaringan komunikasi dengan peralatan listrik yang dimungkinkan dapat dikontrol, dimonitor atau diakses dari jarak jauh. *Smart home* juga dapat meningkatkan efisiensi, kenyamanan dan keamanan dengan menggunakan teknologi secara otomatis [6]. Secara garis besar, *smart home* diciptakan untuk memudahkan pemilik atau penghuni rumah dalam mengatur dan mengontrol beberapa perangkat elektronik supaya dapat bekerja secara otomatis serta dapat diakses dari jarak jauh.

2.2.2 *Face Detection*

Face detection atau pengenalan wajah merupakan teknologi komputer yang digunakan beberapa sistem dan atau aplikasi untuk mendeteksi wajah. Teknologi *face detection* dibangun dengan algoritma tertentu yang berfokus pada deteksi dari wajah manusia. Di dalam teknologi pengenalan wajah, *face detection* merupakan tahap awal pemrosesan untuk mengenali wajah seseorang, dimana *face detection* menentukan dimana bagian wajah yang muncul pada citra masukan[12].

2.2.3 *Face Recognition*

Face recognition atau pengenalan wajah adalah proses mengenali wajah seseorang dimana otak berusaha menginterpretasi, memahami, dan menafsirkan wajah yang ada di hadapannya terutama wajah manusia[8]. *Face recognition* merupakan salah satu teknologi biometrik yang banyak diaplikasikan khususnya dalam sistem *security*[14]. *Face recognition* digunakan untuk mengenali wajah seseorang berdasarkan data gambar wajah yang disimpan dalam *database*. Data-data tersebut dicocokkan berdasarkan citra digital yang kemudian dicari nilai tengah kemiripan wajah yang terinput sekarang dengan wajah yang ada di *database*. dalam penggunaan dibutuhkan kamera sebagai penangkap citra digital berdasarkan video.

Face recognition Secara umum sistem pengenalan wajah dibagi menjadi 2 jenis, yaitu sistem *feature based* dan sistem *imagebased*. Pada sistem pertama fitur lokal didapat dari proses ekstraksi komponen citra wajah seperti mulut, hidung, mata, pipi dan lain-lain. Kemudian dimodelkan secara geometris hubungan antar fitur-fitur tersebut. Sedangkan untuk sistem yang kedua menggunakan informasi mentah dari *pixel* citra yang kemudian direpresentasikan dalam metode tertentu, misalnya *Principal Component Analysis*, transformasi Wavelet, dan sebagainya, yang kemudian digunakan untuk pelatihan dan klasifikasi identitas citra[15].

2.2.4 **OpenCV**

Open Source Computer Vision Library (OpenCV), adalah sebuah library *open source* yang dikembangkan oleh intel yang fokus untuk menyederhanakan programing terkait citra digital[16]. Computer Vision merupakan salah satu cabang dari bidang *Image Processing* (pengolahan citra), yang bekerja layaknya manusia dengan memiliki kecerdasan buatan (*Artificial Intelligent*). Beberapa implementasi *computer vision* diantaranya *Face*

recognition, face detection, face/object tracking, dll[17]. *OpenCV* merupakan *library* yang dapat membuat sistem bekerja secara *real-time*.

2.2.5 Eigenface

Kata *Eigenface* berasal dari Bahasa Jerman “*eigenwert*” dimana “*eigen*” artinya karakteristik dan “*wert*” artinya nilai. *Eigenface* merupakan algoritma pengenalan wajah yang berdasarkan pada *Principle Component Analysis (PCA)*[18]. *Eigenface* merupakan sekumpulan informasi unik wajah berdasarkan dari nilai karakteristik yang dimiliki oleh setiap wajah. Metode *Eigenface* adalah bagaimana cara menguraikan informasi yang relevan dari sebuah citra wajah, kemudian mengubahnya ke dalam satu set kode yang paling efisien dan membandingkan kode wajah tersebut dengan *database* berisi beragam wajah yang telah dikodekan secara serupa [19].

Adapun penghitungan metode *Eigenface* dilakukan dengan beberapa tahap diantaranya yaitu[20]:

1. Langkah pertama, menyusun himpunan matriks (S) yang terdiri dari seluruh *training image* (Γ).

$$S=(\Gamma_1, \Gamma_2, \dots, \Gamma_M) \dots \dots \dots (2.1)$$

2. Dari sekumpulan himpunan matriks, kemudian menentukan nilai tengah / *mean* (ψ) dari kumpulan matriks tersebut.

$$\Psi = \frac{1}{M} \sum_{n=1}^M \Gamma_n \dots \dots \dots (2.2)$$

Dimana banyaknya data *training* (M) dijumlah perulangan (\sum) sebanyak *training image* (Γ) ke -n.

3. Hitung selisih (Φ) antara *training image* (Γ_i) dengan nilai tengah (ψ), dengan cara *training image* (Γ) dikurangi dengan nilai tengah (ψ)

$$\phi_i = \Gamma_i - \Psi \dots \dots \dots (2.3)$$

4. Menghitung matriks kovarian (C) untuk memperoleh nilai *eigenvalue* (λ) dan *eigenvector* (v).

$$C = \frac{1}{M} \sum_{n=1}^M \Phi_n \Phi_n^T = AA^T \dots \dots \dots (2.4)$$

Dikarenakan ukuran matriks terlalu besar maka penghitungan matriks kovarian menjadi

$$C = A^T A \dots \dots \dots (2.5)$$

Dimana matriks selisih (A) diubah transpose (T) dikalikan dengan matriks selisih (A).

5. Menghitung *eigenvalue* (λ) dan *eigenvector* (v) dari matriks kovarian (C)

$$C \times v_i = \lambda_i \times v_i \dots \dots \dots (2.6)$$

Dimana matriks kovarian (C) dikalikan dengan *eigenvector* (v), dan *eigenvalue* (λ) dikalikan dengan *eigenvector* (v).

6. Setelah mendapat *eigenvector* (v), maka langkah selanjutnya mencari *Eigenface* (μ) dengan rumus

$$\mu_i = \sum_{k=1}^M v_{ik} \phi_k \dots \dots \dots (2.7)$$

Dimana *Eigenface* di cari melalui nilai *eigenvector* (v) dikalikan dengan nilai matriks selisih (Φ).

Untuk proses pengenalan wajah dilakukan dengan cara sebagai berikut:

1. Percobaan mengenali *image* wajah baru (Γ_{new}), pertama menerapkan perhitungan *Eigenface* (μ) untuk mendapatkan nilai *eigen* dari *image* tersebut.

$$\mu_{new} = v \times (\Gamma_{new} - \Psi), \Omega = [\mu_1, \mu_2, \dots, \mu_M] \dots \dots \dots (2.8)$$

Dimana *Eigenface* baru (μ_{new}) dihasilkan dari *eigenvector* (v) dikali hasil nilai tengah (ψ) *image* baru (Γ_{new}). Dan omega (Ω) merupakan himpunan matriks *Eigenface* (μ).

2. Menggunakan metode *Euclidean distance* untuk mencari jarak terpendek antara nilai *eigen* dari data *training* dengan nilai *eigen* *image* wajah baru.

$$\epsilon_k = ||\Omega - \Omega_k|| \dots \dots \dots (2.9)$$

Dimana jarak terpendek dengan menggunakan *Euclidean distance* didapat dengan cara rentang nilai *Eigenface training image* (μ) dikurangi dengan nilai *Eigenface test image* (μ_{new}).

Eigenface memiliki beberapa kelemahan diantaranya yaitu ketika cahaya yang didapat berbeda sehingga pada saat mencari kemiripan akan mendeteksi orang yang berbeda, padahal dalam mata manusia itu merupakan orang yang sama. Hal ini terjadi karena bedanya citra digital yang didapat oleh komputer pada saat pencocokan wajah. Beberapa faktor kelemahan *Eigenface* diantaranya yaitu: gambar stretch, blur, ekspresi wajah yang berbeda, dan perubahan latar belakang objek yang dideteksi seperti misalnya terjadi perubahan cuaca.

2.2.6 Principal Component Analysis (PCA)

Principal Component Analysis (PCA) merupakan transformasi linier yang biasa digunakan dalam mereduksi data. *Principal Component Analysis (PCA)* yaitu suatu teknik analisis faktor di mana beberapa faktor yang akan terbentuk berupa variabel laten yang belum dapat ditentukan sebelum analisis dilakukan. Pada prinsipnya analisis faktor eksploratori di mana terbentuknya faktor-faktor atau variabel laten baru adalah bersifat acak, yang selanjutnya dapat diinterpretasi sesuai dengan faktor atau komponen atau konstruk yang terbentuk. PCA merupakan suatu teknik untuk mereduksi data dari variabel asal atau variabel awal menjadi variabel baru atau faktor yang jumlahnya lebih kecil dari pada variabel awal [21].

2.2.7 Support Vector Machine (SVM)

Support Vector Machine (SVM) adalah algoritma yang bekerja dengan menggunakan pemetaan non linier untuk mengubah data *training* ke dimensi yang lebih tinggi [22]. *Support Vector Machine (SVM)* merupakan salah satu metode *Supervised Machine Learning* yang banyak digunakan untuk proses

klasifikasi dan analisis regresi [23]. *Support Vector Machine* membentuk suatu *hyperplane* pada dimensi jarak yang tinggi, secara garis besar pemilahan terbaik yang dicapai oleh *hyperplane* yang memiliki jarak terbesar ke titik data *training* terdekat dari setiap *class*. Semakin besar *class* maka semakin kecil tingkat error pada klasifikasi.

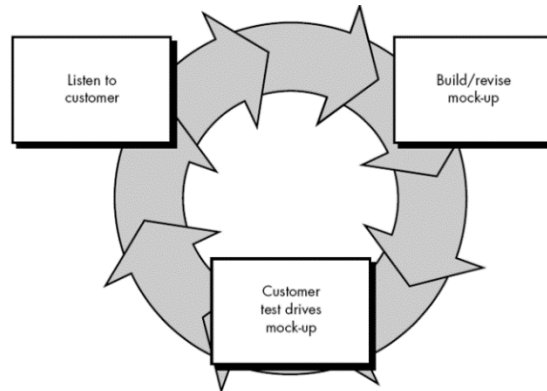
Langkah-langkah pengklasifikasian dengan *Support Vector Machine (SVM)*.

1. Data *training* digunakan, setiap model klasifikasi ke-I *training* dengan menggunakan keseluruhan data
2. Setelah dilakukan *training* dan mendapatkan klasifikasi, tahap selanjutnya menguji klasifikasi data *training* dengan data *test*. Untuk mendapatkan nilai akurasi [22].

2.2.8 System Development Live Cycle (SDLC)

System Development Live Cycle atau lebih familiar disebut dengan SDLC merupakan metodologi yang digunakan dalam pembuatan suatu sistem[24]. SDLC adalah siklus dalam pengembangan suatu sistem informasi dengan tujuan menyelesaikan masalah dan efektivitas dari pengembangan tersebut [25]. SDLC terdiri dari beberapa tahapan, yang dimulai dari tahapan perencanaan, analisis, perancangan, implementasi, dan pengujian. Terdapat berbagai macam model dari metode SDLC, salah satu yang sering digunakan yaitu model *waterfall* dan *prototype*.

Pada penelitian ini menggunakan metode pengembangan SDLC model *prototype*. Pengembangan sistem perangkat lunak model *prototype* merupakan salah satu model dimana pengguna memiliki gambaran garis besar dari sebuah sistem yang dikembangkan[26].



Gambar 2.1 Tahapan SDLC *Prototype*

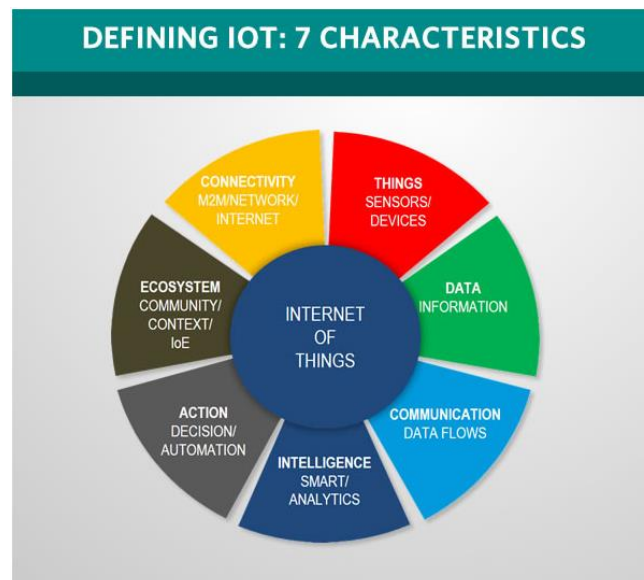
Tahapan-tahapan dari pengembangan model *prototype* sebagai berikut :

1. Pengumpulan kebutuhan, pada tahapan ini merupakan analisa dari kebutuhan pada pengembangan sistem.
2. Membangun *prototype*, tahapan ini merupakan perancangan keseluruhan sistem yang akan dibuat dengan memuat berbagai aspek pengembangan sistem. Seperti perancangan mockup maupun jalan alur dari sistem.
3. Evaluasi *prototype*, pada tahapan ini merupakan tahapan evaluasi dari perancangan *prototype*.
4. Pengkodean sistem, tahapan ini merupakan implementasi komputerisasi dari perancangan yang telah dibuat sebelumnya.
5. Pengujian sistem, tahapan ini merupakan tahapan final dari semua tahapan dari pengembangan. Sistem diuji secara berkala untuk mengetahui suatu sistem berjalan sesuai dengan harapan[26].

Penggunaan SDLC model *prototype* pada penelitian ini sangat cocok. Hal ini didasari oleh tahapan-tahapan pemodelan *prototype* pada pengembangan sistem keamanan rumah sesuai dengan ide penelitian ini dimana pada penelitian ini menghasilkan produk berupa perangkat yang terintegrasi dengan website.

2.2.9 *Internet of Things*

Internet of Things (IoT) merupakan kumpulan benda-benda (*things*), berupa perangkat fisik (*hardware /embedded system*) yang mampu bertukar informasi antar sumber informasi, operator layanan ataupun perangkat lainnya yang terhubung kedalam sistem sehingga dapat memberikan kemanfaatan yang lebih besar. Perangkat fisik (*hardware/embedded system*) dalam infrastruktur *Internet of Things* merupakan *hardware* yang tertanam (*embedded*) dengan elektronik, perangkat lunak, sensor dan juga konektivitas [10]. *Internet of Things* dalam penerapannya juga dapat mengidentifikasi, menemukan, melacak, memantau objek dan memicu event terkait secara otomatis dan real time, Pengembangan dan penerapan komputer, *Internet* dan teknologi informasi dan komunikasi lainnya (TIK) membawa dampak yang besar pada masyarakat manajemen ekonomi, operasi produksi, sosial manajemen dan bahkan kehidupan pribadi [27].



Gambar 2.2 Defining IoT using 7 characteristic.[28]

Tujuh karakteristik penting dari *Internet of Things*, di antaranya sebagai berikut: *Connectivity* (konektivitas) merupakan koneksi antara perangkat dan

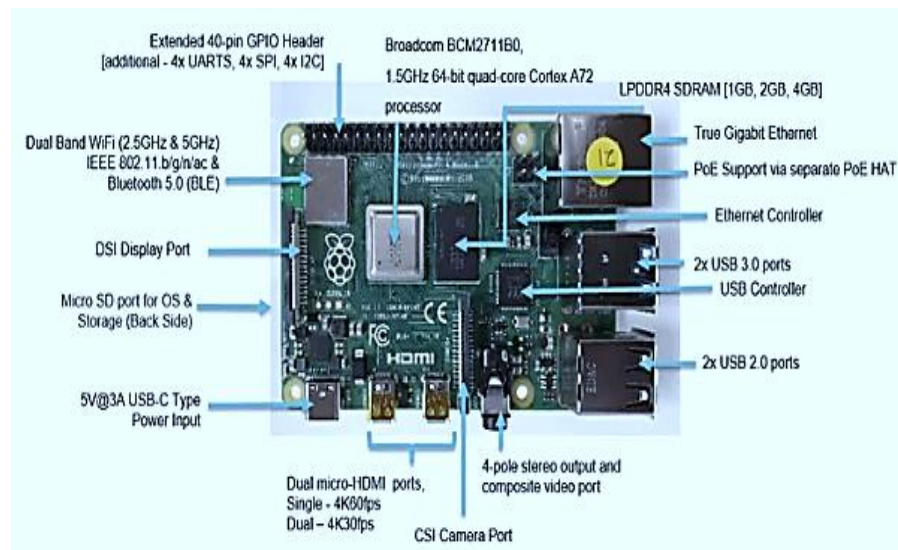
sensor ke suatu item satu sama lain, *actuator*, maupun suatu proses ke internet atau jaringan yang lainnya. *Things*, apapun yang yang dapat dihubungkan. Mulai dari sensor dan peralatan rumah tangga serta perangkat penginderaan yang dapat terikat satu sama yang lainnya. Data merupakan perekat *Internet of Things*, langkah pertama menuju aksi atau tindakan dan kecerdasan. *Communication*, perangkat dapat terhubung sehingga bisa saling berkomunikasi, bertukar data dan dapat menganalisa data yang didapat. *Intelligence*, aspek kecerdasan meliputi kemampuan penginderaan dalam perangkat IoT dan kecerdasan dikumpulkan serta dianalisis data yang termasuk kecerdasan buatan. *Action*, beberapa tindakan yang dilakukan sensor untuk mengambil data, bisa berupa tindakan manual, tindakan berdasarkan studi kasus (misalnya pengambilan keputusan), dan tindakan otomatis. *Ecosistem*, tempat *Internet of Things* dari perspektif teknologi lain, komunitas, tujuan dan gambar di mana *Internet of Things* cocok. Dimensi *Internet of Things*, dimensi *platform*, dan kebutuhan akan kemitraan yang solid. [28]

2.2.10 Raspberry Pi

Raspberry Pi adalah sebuah komputer mini yang biasa disebut sebagai *Single Board Computer (SBC)*. Raspberry Pi memiliki ukuran yang kecil hampir menyerupai besarnya kartu KTP, ATM, dll. Raspberry Pi didirikan oleh Raspberry Pi Foundation yang merupakan sebuah badan amal yang bertempat di Inggris dengan tujuan mengenalkan ketrampilan komputer kepada orang – orang di seluruh dunia. Sehingga lebih banyak orang dapat memanfaatkan komputasi dan teknologi digital untuk bekerja, memecahkan masalah, dan mengekspresikan diri [29].

Proyek Raspberry Pi dimulai pada tahun 2006. Para pendiri ingin merasakan semangat menjadi perintis komputasi, seperti yang dirasakan pada tahun 1980-an, ketika komputer pribadi yang terjangkau tersedia untuk penggemar atau pemula yang sedang tumbuh[30]. Sejak proyek Raspberry Pi

dilaunching secara umum dari tahun 2012 hingga sekarang, telah menciptakan 9 produk *single board computer* diantaranya yaitu : Raspberry Pi Zero, Raspberry Pi Zero W, Raspberry Pi 1 model A+, Raspberry Pi 1 model B+, Raspberry Pi 2 model B, Raspberry Pi 3 model B, Raspberry Pi 3 model A+, Raspberry Pi 3 model B+, dan Raspberry Pi 4 model B. Perbedaan antara model A dan B terletak pada port LAN, dimana pada model A port ini tidak tersedia. kemudian pada model A, RAM yang digunakan tidak sebesar pada model B. Rentang tegangan yang dibutuhkan Raspberry Pi 4 model B sebesar 5 Volt atau 3 Ampere. Raspberry Pi 4 model B merupakan versi terbaru yang diluncurkan. Berikut susunan struktur input/output Raspberry Pi 4 model B :



Gambar 2.3 Raspberry Pi 4 model B[31].

Dari gambar diatas Raspberry memiliki processor dengan kecepatan sebesar 1,5 GHz, dengan pilihan RAM mulai dari 1 GB, 2GB, dan 4GB. Selain itu untuk mendukung beberapa proyek *Internet of Things*, Raspberry Pi memiliki 40 pin *General Purpose Input Output* (GPIO), dimana pin ini berfungsi sebagai input output sebuah sensor yang ditancapkan. Konektor GPIO memiliki fitur-fitur diantaranya sebagai berikut:

- a. Pin antarmuka I²C yang memungkinkan untuk menghubungkan modul hardware dengan hanya dua pin control.
- b. SPI, memiliki konsep mirip dengan I²C dengan standar yang berbeda.
- c. Serial Rx dan Tx, pin untuk berkomunikasi dengan perangkat serial.
- d. Pin *Pulse Width Modulation* (PWM) untuk control daya.
- e. Pin *Pulse Position Modulation* (PPM) untuk mengendalikan motor servo.
- f. GND, Pin ground atau arus negatif untuk sensor.
- g. Pin 5V dan 3V, pin tegangan arus yang dialirkan ke sensor [32].

2.2.11 MySQL

MySQL adalah manajemen basis data yang menggunakan perintah dasar *Structured Query Language* (SQL). MySQL adalah *database server* yang gratis, sehingga dapat digunakan secara personal maupun komersil[33]. MySQL termasuk kedalam *Relational Database Management System* (RDBMS), dimana dalam strukturnya menggunakan tabel yang saling berelasi. MySQL memiliki fungsi sebagai pembuat dan pengelola *database* pada sisi *server* yang memuat berbagai informasi suatu sistem atau *website*. PHPMyAdmin merupakan *server* yang biasa digunakan MySQL untuk menghubungkan dengan pemrograman berbasis PHP [34].

2.2.12 Bahasa Pemrograman Python

Python adalah bahasa pemrograman interpretatif multiguna dengan filosofi perancangan yang berfokus pada tingkat keterbacaan kode. Bahasa pemrograman python disebut sebagai bahasa yang memiliki kemampuan menggabungkan kapabilitas dan sintaksis kode yang sangat jelas, dan juga dilengkapi dengan fungsionalitas pustaka standar yang besar serta komprehensif[35]. Python merupakan bahasa pemrograman tingkat tinggi yang telah menjadi standar dalam duni komputasi ilmiah. Python merupakan bahasa

pemrograman *open source multi platform* yang dapat digunakan pada berbagai macam sistem operasi seperti Windows, Linux, dan MacOS.

Bahasa pemrograman Python dalam banyak hal berbeda dengan bahasa pemrograman *procedural* seperti C, C++, dan Fortran. Dalam ketiga bahasa pemrograman *procedural* tersebut, file *source code* harus dikompilasi ke dalam bentuk *executable file* sebelum dijalankan. Pada python tidak terdapat langkah kompilasi, sebagai gantinya *code* ditulis secara langsung baris demi baris. Kelebihan bahasa python adalah tidak membutuhkan pendeklarasian variabel, sehingga lebih fleksibel dalam penggunaannya. Namun terdapat kelemahan pada python yakni program – program numerik dijalankan pada python lebih lambat ketimbang dijalankan menggunakan bahasa yang menganut kompilasi [36].

2.2.13 Flask

Flask merupakan sebuah web *framework* yang ditulis dengan bahasa pemrograman Python dan termasuk ke dalam jenis *microframework*. Dengan menggunakan Python, flask dapat membuat suatu web secara terstruktur dan mudah. Flask disebut *microframework* dikarenakan tidak memerlukan *library* maupun ekstensi – ekstensi yang berlebihan. Sebagian besar fungsi dan komponen, seperti validasi form, *database*, dan sebagainya tidak terpasang secara default di flask. Hal ini memudahkan *developer* dalam membangun suatu web, yang dapat menggunakan ekstensi secara bebas dari pihak ketiga. Saat mengakses web berbasis flask maka pengguna akan merasakan ringan, hal ini dikarenakan flask memiliki *core* yang sederhana serta dapat menangani fungsi HTTP *request* yang cepat [37].

2.2.14 Black Box Testing

Black box testing merupakan pengujian fungsional dari suatu sistem tanpa mengetahui *internal* kode pemrograman. Pengujian *black box* didasarkan

pada pengujian tampilan aplikasi, menu aplikasi, dan fungsi-fungsi pada aplikasi [38]. *Black box testing* atau pengujian fungsionalitas merupakan pengujian perangkat lunak tanpa mengetahui struktur kode dan bahasa pemrograman yang digunakan [39]. Adapun beberapa kelebihan dan kelemahan dalam pengujian dengan menerapkan *black box* yaitu:

Kelebihan dalam menggunakan *black box* yaitu:

1. Lebih ringkas dalam pengujian pada suatu sistem yang kompleks
2. Tidak memerlukan akses kode suatu sistem
3. Dapat memilah atau memisah pengujian dari sudut pandang pengguna dan pengembang.

Kelemahan dalam pengujian *black box* yaitu:

1. Cakupan pengujian tidak luas, hanya sebatas *interface* dan fungsi sistem
2. Diperlukan pengetahuan dari penguji
3. Tidak menguji *backend* [39].