KUNCI KESELAMATAN ANTARA MUKA PENGATURCARAAN APLIKASI (API) PADA SISTEM PAPAN PEMUKA BAGI PERISIAN TENGAHINTERNET BENDA (IOT)

Mohd Jalaluddin Ahmad
Mohamad Faidzul Nasrudin
Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

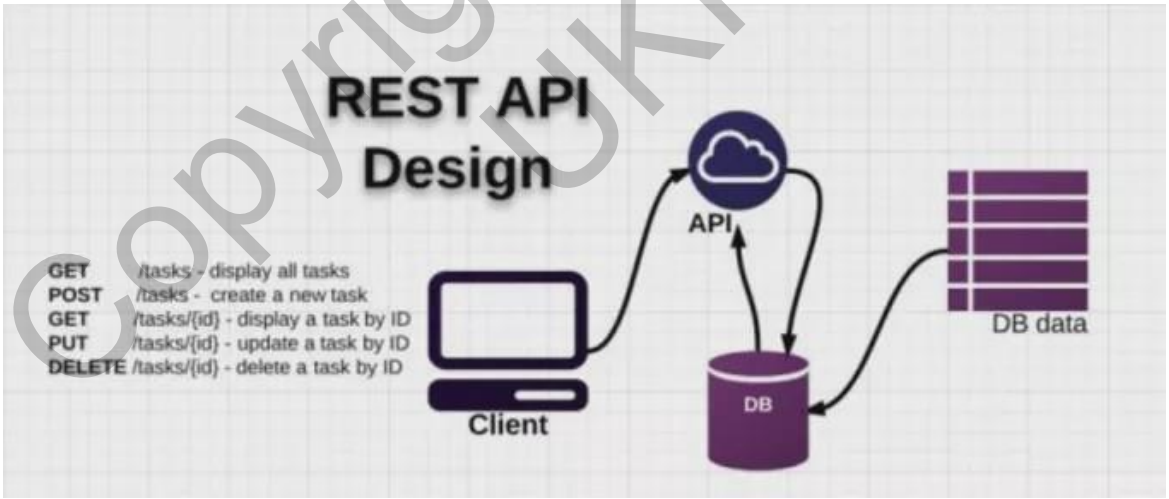
ABSTRAK

Antara muka pengaturcaraan aplikasi (API) merupakan sub-rutin protokol komunikasi dan sebahagian dari alat membina perisian. Menulis kod atur cara bagi antara muka pengaturcaraan aplikasi (API) lebih mudah berbanding dengan komponen bahasa pengaturcaraan lain dengan penyediaan blok permintaan antara muka pengaturcaraan aplikasi (API) yang terdiri dari *get*, *post*, *patch*, *put* dan *delete*. Penggunaan antara muka pengaturcaraan aplikasi (API) sama seperti antara muka grafik pengguna (GUI) di mana akan memudahkan pengguna menggunakan program, namun antara muka pengaturcaraan aplikasi (API) lebih digunakan oleh pembangun sistem berbanding pengguna akhir. Pengurusan antara muka pengaturcaraan aplikasi (API) membantu pembangun sistem dalam memastikan data sentiasa selari dan mudah dicapai. Kebolehan antara muka pengaturcaraan aplikasi (API) mengakses terus kepada sistem pangkalan data menggunakan blok permintaan tertentu mengakibatkan risiko manipulasi data terus kepada pangkalan data yang akan mengakibatkan toleransi kesalahan dan integriti data tidak terkawal. antara muka pengaturcaraan aplikasi (API) tidak menyediakan sebarang kaedah kawalan pengurusan capaian data dan kawalan ini perlu di buat oleh pembangun sistem sepenuhnya. Mengenal pasti supaya tidak berlakunya risiko manipulasi data hasil dari cubaan melalui blok permintaan antara muka pengaturcaraan aplikasi (API) yang mudah untuk berinteraksi terus dengan pangkalan data. Menggunakan kaedah toleransi melalui kunci peribadi diantara pangkalan data dengan hanya mengenal pasti hanya kunci peribadi yang sama sahaja mempunyai kebolehan melakukan blok permintaan antara muka pengaturcaraan aplikasi (API). Kaedah kunci peribadi menghasilkan tahap keselamatan asas di mana permintaan antara muka pengaturcaraan aplikasi (API) perlu sama dengan kunci peribadi pada pangkalan data. Kunci peribadi tersebut boleh ditambah baik menggunakan konsep fungsi *Blockchain* atau sebarang kaedah kriptologi lain yang bersesuaian namun memerlukan perkakasan khas bagi membolehkan fungsi berjalan.

1. PENGENALAN

Menulis kod atur cara bagi antara muka pengaturcaraan aplikasi (API) lebih mudah berbanding dengan komponen bahasa pengaturcaraan lain dengan penyediaan blok permintaan antara muka pengaturcaraan aplikasi (API) yang terdiri dari *get*, *post*, *patch*, *put* dan *delete*. Penggunaan antara muka pengaturcaraan aplikasi (API) sama seperti antara muka grafik pengguna (GUI) di mana akan memudahkan pengguna menggunakan program, namun antara muka pengaturcaraan aplikasi (API) lebih digunakan oleh pembangun sistem berbanding pengguna akhir.

REST API merupakan sebahagian dari antara muka pengaturcaraan aplikasi (API) dengan singkatan REST (*Representional State Transfer*) adalah sebuah kaedah komunikasi yang menggunakan protokol permintaan HTTP untuk penghantaran data dimana kaedah ini sering diterapkan dalam pengembangan aplikasi. Dengan tujuannya untuk menjadikan sistem memiliki performa yang baik, cepat dan mudah untuk di kembangkan *(scale)* terutama dalam penghantaran dan komunikasi data.



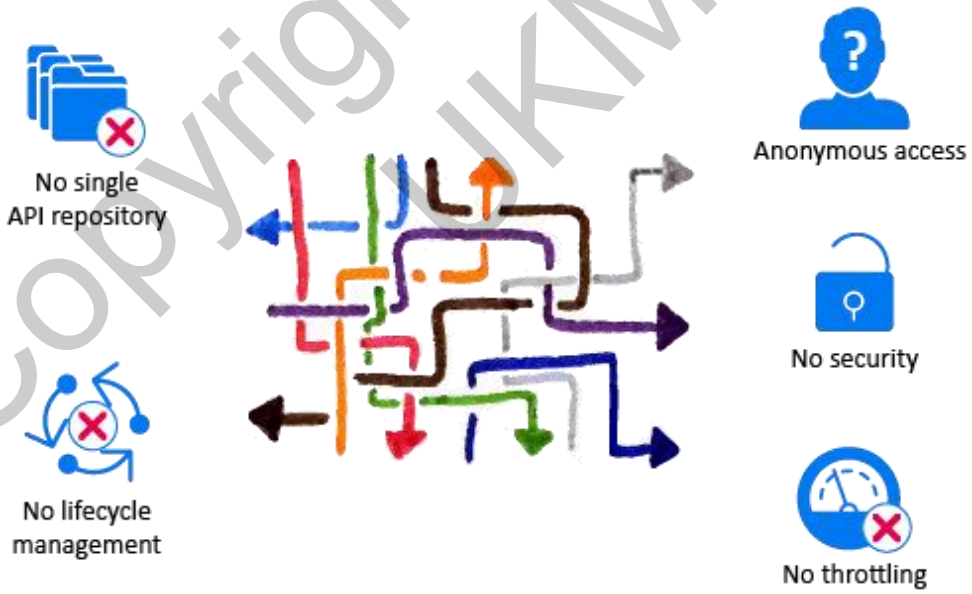
Rajah 1.1 – Reka Bentuk REST API

Sistem Papan Pemuka Bagi Perisian Tengah Internet Benda (IoT) menggunakan kerangka Laravel yang telah dilengkapi dengan antara muka pengaturcaraan aplikasi (API). Fungsi antara muka pengaturcaraan aplikasi (API) digunakan sebagai perantara antara peranti Internet Benda (IoT) dengan sistem Sistem Papan Pemuka Bagi Perisian Tengah Internet Benda (IoT).

2. PENYATAAN MASALAH

Kebolehan antara muka pengaturcaraan aplikasi (API) mengakses terus kepada sistem pangkalan data menggunakan blok permintaan tertentu mengakibatkan risiko manipulasi data terus kepada pangkalan data yang akan mengakibatkan toleransi kesalahan dan integriti data tidak terkawal. Antara muka pengaturcaraan aplikasi (API) tidak menyediakan sebarang kaedah kawalan pengurusan capaian data dan kawalan ini perlu di buat oleh pembangun sistem sepenuhnya.

Risiko akses secara terbuka daripada pengguna yang tidak dikenali mampu mengakibatkan kegagalan tahap keselamatan pada pangkalan data atau sesuatu sistem aplikasi. Selain itu, antara muka pengaturcaraan aplikasi (API) tidak dibina dengan repositori yang membolehkan pemantauan di buat serta kitaran hayat antara muka pengaturcaraan aplikasi (API) yang tidak tersusun menyebabkan antara muka pengaturcaraan aplikasi (API) merupakan ruang terbuka bagi sesiapa sahaja yang memerlukan data terus dari sesuatu sistem aplikasi.



Rajah 2.1 – Lakaran Masalah antara muka pengaturcaraan aplikasi (API)

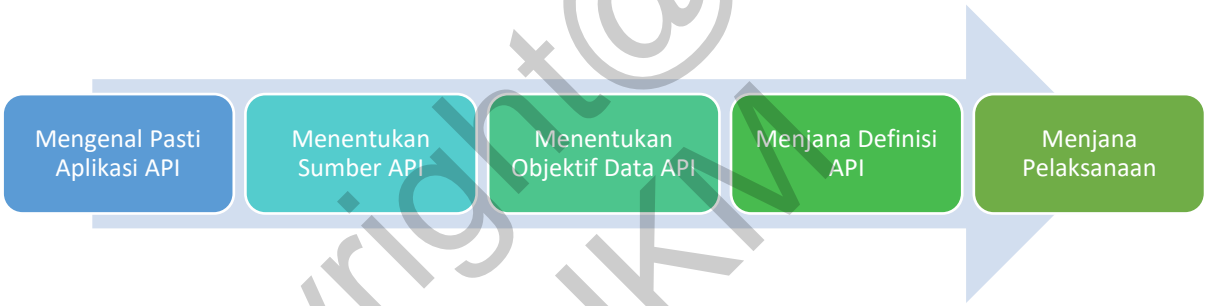
Antara muka pengaturcaraan aplikasi (API) boleh diakses melalui fungsi yang ditetapkan dalam kerangka Laravel pada Sistem Papan Pemuka Bagi Perisian Tengah Internet Benda (IoT). Fungsi antara muka pengaturcaraan aplikasi (API) yang ada hanya fungsi asas dengan tanpa kawalan keselamatan pada setiap permintaan API yang di buat.

3. OBJEKTIF KAJIAN

Sistem Papan Pemuka Bagi Perisian Tengah Internet Benda (IoT) dibangunkan dengan fungsi antara muka pengaturcaraan aplikasi (API) bagi mencapai objektif dalam perantara antara peranti Internet Benda (IoT) dengan sistem seperti berikut:

- Keberkesanan permintaan pengurusan data antara muka pengaturcaraan aplikasi (API)
- Membangun algoritma kunci keselamatan bagi pengesahan permintaan antara muka pengaturcaraan aplikasi (API)

4. METODOLOGI KAJIAN



Rajah 4.1 – Aliran Pembangunan Antara Muka Pengaturcaraan Aplikasi (API)

Merujuk Rajah 4.1 merupakan aliran bagi pembangunan penggunaan fungsi antara muka pengaturcaraan aplikasi (API) dalam Sistem Papan Pemuka Bagi Perisian Tengah Internet Benda (IoT). Menggunakan kaedah toleransi melalui kunci peribadi diantara pangkalan data dengan hanya mengenal pasti hanya kunci peribadi yang sama sahaja mempunyai kebolehan melakukan blok permintaan API.

4.1 Fasa Perancangan

Sistem Papan Pemuka Bagi Perisian Tengah Internet Benda (IoT) menggunakan antara muka pengaturcaraan aplikasi (API) dalam aliran data antara peranti Internet Benda (IoT) dengan sistem aplikasi. Mencipta satu algoritma kunci peribadi pada antara muka pengaturcaraan aplikasi (API) sebagai fungsi pengesahan proses permintaan yang dibuat.

Mengenal pasti aplikasi antara muka pengaturcaraan aplikasi (API) adalah kaedah merancang penggunaan antara muka pengaturcaraan aplikasi (API) yang bersesuaian sebelum penulisan algoritma dibuat.

4.2 Fasa Analisis

Satu pengujian ringkas dalam proses permintaan antara muka pengaturcaraan aplikasi (API) dalam proses mendapatkan maklumat melalui permintaan. Pemerhatian daripada proses ringkas tersebut mendapati dengan menambah kunci peribadi sebagai sebahagian fungsi keselamatan adalah amat baik dalam memastikan tiada kebocoran atau manipulasi data kepada pengguna yang tidak dikenali.

Menentukan sumber antara muka pengaturcaraan aplikasi (API) di mana fungsi pertanyaan terus ke pangkalan data di pilih mengikut keperluan permintaan pengguna. Penentuan keperluan pembangunan kunci peribadi juga di buat dalam mencapai objektif fungsi kunci peribadi antara muka pengaturcaraan aplikasi (API).

4.3 Fasa Reka Bentuk

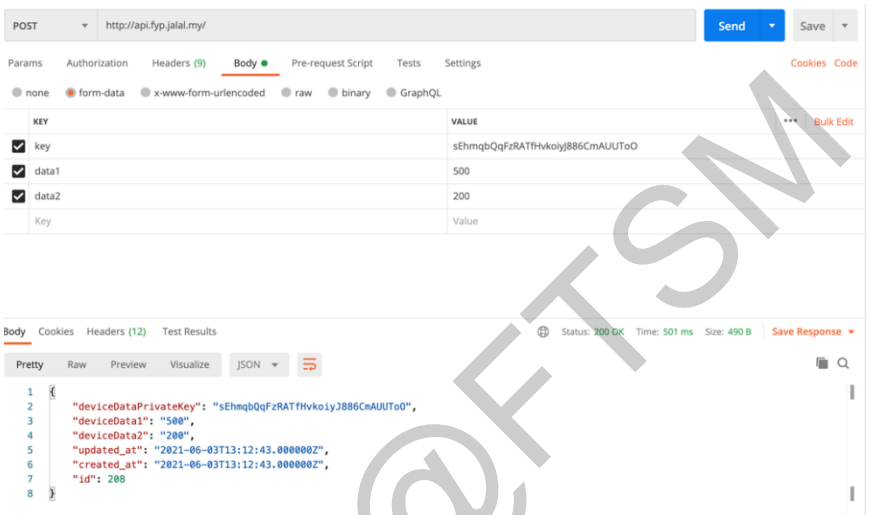
```
Terima Kunci Peribadi
Uji Kunci Peribadi dengan Maklumat Kunci dalam pangkalan data
Jika sama lakukan
    Melaksanakan permintaan berdasarkan input
Jika tidak sama lakukan
    Mengeluarkan status permintaan
```

Rajah 4.2 – Algoritma Kunci Peribadi

Merujuk kepada rajah 4.2 Algoritma kunci peribadi dibangunkan bagi memastikan kaedah perjalanan fungsi tersebut berjalan dengan lancar. Algoritma ini diletakkan dalam bahagian *controller* antara muka pengaturcaraan aplikasi (API) kerangka Laravel.

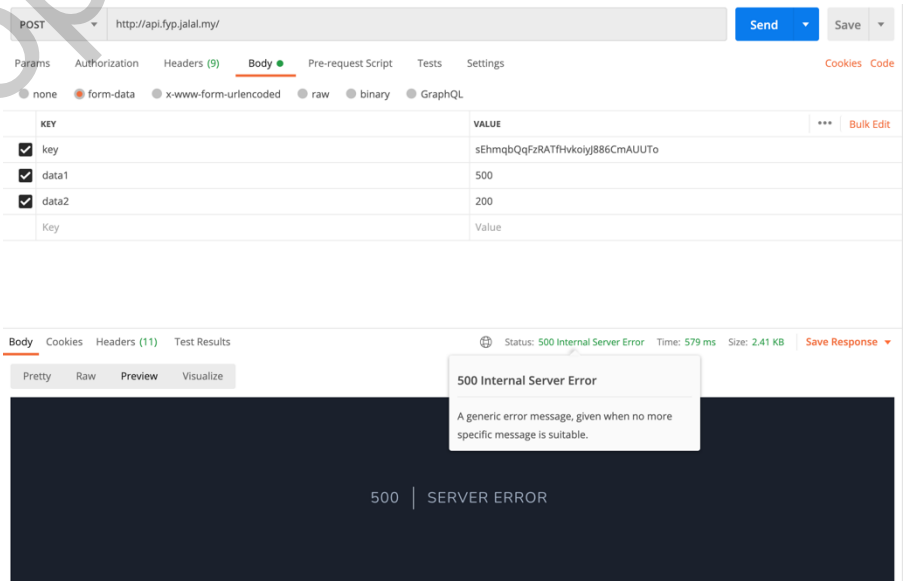
Definisi antara muka pengaturcaraan aplikasi (API) dapat menjadi sebahagian rujukan semasa reka bentuk di buat sebelum dapat menjana kunci peribadi antara muka pengaturcaraan aplikasi (API) dengan lebih berkesan.

4.4 Fasa Pengujian



Rajah 4.3 – Pengujian Kunci Keselamatan (Status Permintaan Berjaya)

Merujuk rajah 4.3 dan rajah 4.4 pengujian di buat menggunakan perisian Postman di mana kemasukan data permintaan yang berjaya dan gagal dipaparkan berdasarkan toleransi kesalahan pada kunci keselamatan mengikut kesamaan di dalam pangkalan data.



Rajah 4.4 – Pengujian Kunci Keselamatan (Status Permintaan Gagal)

5 HASIL KAJIAN

Kaedah kunci peribadi menghasilkan tahap keselamatan asas di mana permintaan antara muka pengaturcaraan aplikasi (API) perlu sama dengan kunci peribadi pada pangkalan data. Algoritma dan fungsi kunci keselamatan dibangunkan yang berfungsi sebagai keselamatan dan pengesahan permintaan antara muka pengaturcaraan aplikasi (API) dalam Sistem Papan Pemuka Bagi Perisian Tengah Internet Benda (IoT). Kunci keselamatan diuji menggunakan perisian Postman dan sistem akan memberikan kod status standard yang dapat digunakan untuk menyampaikan hasil permintaan.

Jadual 5.1 – Senarai Kod Status

KOD STATUS	STATUS	PENERANGAN
1xx	Maklumat	Berkomunikasi memindahkan maklumat tahap protokol.
2xx	Berjaya	Menunjukkan bahawa permintaan pelanggan berjaya diterima.
3xx	Ubah Hala	Menunjukkan bahawa pelanggan mesti mengambil tindakan tambahan untuk menyelesaikan permintaan mereka.
4xx	Kesalahan Pelanggan	Kod status ralat kategori ini menuding klien.
5xx	Ralat Pelayan	Pelayan bertanggungjawab terhadap kod status ralat ini.

Kunci tersebut juga diagihkan kepada dua bahagian iaitu peribadi dan terbuka dimana kunci peribadi mempunyai blok permintaan antara muka pengaturcaraan aplikasi (API) yang terdiri dari *post*, *patch*, *put* dan *delete* manakala kunci terbuka hanya mempunyai blok permintaan antara muka pengaturcaraan aplikasi (API) *get* sahaja.

6 KESIMPULAN

Penggunaan kunci peribadi boleh ditambah baik menggunakan konsep fungsi *Blockchain* atau sebarang kaedah kriptologi lain yang bersesuaian namun memerlukan perkakasan khas bagi membolehkan fungsi berjalan.

7 RUJUKAN

Wikipedia. 2018. Antara muka pengaturcaraan aplikasi. https://ms.wikipedia.org/wiki/Antara_muka_pengaturcaraan_aplikasi

PT Mitra Integrasi Informatika. 2018. Konsep Restful API Programming (Bagian-1). https://www.mii.co.id/en/insight/listing/2021/06/21/03/58/konsep-restful-api-programming-bagian-1

Red Hat. 2020. What is a REST API?. https://www.redhat.com/en/topics/api/what-is-a-rest-api

M. Sabaratnam, O. Torbjornsen and S. -. Hvasshovd, "Evaluating the effectiveness of fault tolerance in replicated database management systems," Digest of Papers. Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing (Cat. No.99CB36352), 1999, pp. 306-313, doi: 10.1109/FTCS.1999.781065.

IBM. RESTful API Design Methodology. https://www.ibm.com/docs/en/ips/8.8?topic=guide-restful-api-design-methodology