

Perancangan Aplikasi Grup Touring Berbasis Mobile Menggunakan Metode Md5

Mobile-Based Touring Group Application Design Using Md5 Method

Salammudin^{*1}, Andi Marwan², Divi Handoko³

^{1,2,3} Fakultas Teknik dan Komputer, Teknik Informatika, Universitas Harapan Medan, Indonesia

E-mail: ¹salammudin2001@gmail.com, ²andimarwanelhanafi@gmail.com, ³divihandoko@gmail.com

Abstrak

Perkembangan teknologi saat ini begitu cepat. Teknologi membuat perubahan pada peradaban manusia. Di era globalisasi saat ini perkembangan teknologi semakin pesat, terutama teknologi internet bahkan saat ini alat telekomunikasi khususnya berbasis mobile sangat membutuhkan akses internet agar mudah terhubung. Grup/Komunitas adalah jaringan dari beberapa individu yang berbentuk kekeluargaan, kemudian saling mengikat dalam meningkatkan sosialisasi sesama jaringan, saling mendukung dan mensupport satu sama lain, memberikan informasi, adanya rasa memiliki persatuan yang erat dan menjadi identitas sosial pengguna kendaraan bermotor. Berdasarkan masalah tersebut dibutuhkan suatu sistem yang dapat menyelesaikan permasalahan tersebut hal inilah yang mendorong penulis merancang Perangkat Lunak untuk memudahkan ketua, anggota dan masyarakat untuk membuat komunitas yang lebih baik lagi.

Kata kunci: Grup, mobile, Aplikasi, MD5, Touring

Abstract

The development of technology today is so fast. Technology makes changes in human civilization. In the current era of globalization, technological developments are increasingly rapid, especially internet technology, even now telecommunication tools, especially mobile-based, really need internet access to be easily connected. Group/Community is a network of several individuals in the form of kinship, then bind each other in increasing the socialization of fellow networks, mutually support and support each other, provide information, have a sense of belonging to a close unity and become the social identity of motorized vehicle users. Based on these problems we need a system that can solve these problems, this is what drives the authors to design software to make it easier for leaders, members and the community to create a better community by raising.

Keywords: Group, mobile, application, MD5, Touring

1. PENDAHULUAN

Perkembangan teknologi saat ini begitu cepat. Teknologi membuat perubahan pada peradaban manusia. Di era globalisasi saat ini perkembangan teknologi semakin pesat, terutama teknologi internet bahkan saat ini alat telekomunikasi khususnya berbasis mobile sangat membutuhkan akses internet agar mudah terhubung. Internet adalah menyangkut komunikasi diseluruh dunia melalui jaringan komunikasi elektronik yang dimungkinkan karena adanya konektivitas jaringan komputer[1]. Oleh karena itu hal tersebut dapat dimanfaatkan untuk membantu aktivitas touring. Telah banyak kegiatan manusia yang didukung kemajuan teknologi. Tak terkecuali kegiatan *touring* yang dilakukan bersama-sama. Touring menjadi agenda bagi

sebagian komunitas motor yang mana dengan demikian biasanya touring di lakukan secara berkelompok. Komunitas touring dalam melakukan aktifitas touring mereka selalu berinteraksi dengan alat komunikasi seperti handphone, handphone sangat penting untuk di bawa saat touring, selain barang-barang yang penting lainnya, permasalahan yang sering terjadi adalah ketika menggunakan handphone tidak adanya aplikasi grup touring.

Pada titik muncul masalah yang dihadapi adalah tidak adanya suatu sistem yang dibuat untuk memberikan informasi kegiatan, touring, semua informasi dikirim melalui chat grup yang dimana belum tentu sempat dibaca oleh anggota dan pengurus terkait, hal ini mengakibatkan kurang komunikasi dan kekompakan antar anggota club motor dan menimbulkan perpecahan, oleh karena itu penulis membuat aplikasi untuk membantu permasalahan pada club motor tersebut.

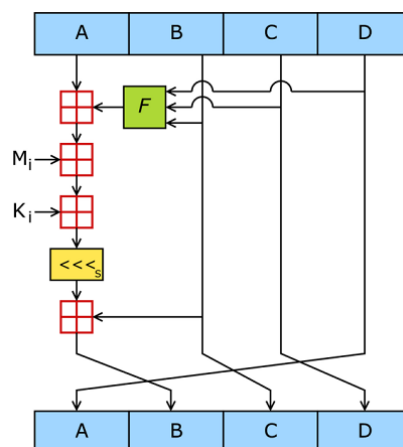
2. METODE PENELITIAN

2.1 Metode MD-5

Setiap pesan yang akan dienkripsi, terlebih dahulu dicari berapa banyak bit yang terdapat pada pesan. Diumpamakan sebanyak 8 bit. Di sini b adalah bit non negatif integer, bisa saja nol dan tidak harus selalu kelipatan delapan. Fungsi hash adalah fungsi yang melakukan pemetan pesan dengan panjang sembarang ke sebuah teks khusus yang disebut message digest dengan panjang tetap. Fungsi hash dapat menerima masukan string apa saja, jika string menyatakan pesan (message), maka sembarang pesan M berukuran bebas dikompresi oleh fungsi H melalui persamaan algoritma berikut:

$$h = H(M) \dots \dots \dots (1)$$

Pada persamaan (1), h adalah nilai hash atas message digest dari H untuk masukan M . Dengan kata lain fungsi hash mengonversikan sembarang pesan yang ukurannya selalu tetap. Algoritma MD5 dirancang Ron Rivest dan penggunaanya sangat populer dikalangan komunitas open source sebagai checksum untuk file yang dapat di download. Besarnya blok untuk MD5 adalah 512 bit sedangkan digest size adalah 128 bit. MD5 mengolah blok 512 bit, dibagi ke dalam 16 blok berukuran 32 bit. Keluaran algoritma diset menjadi 4 blok yang masing-masing berukuran 32 bit yang setelah digabungkan akan membentuk nilai hash 128 bit. MD5 terdiri atas 64 operasi, dikelompokkan dalam empat putaran dari 16 operasi proses[2].



Gambar 1 Satu Operasi MD5

3. HASIL DAN PEMBAHASAN

3.1 Langkah-Langkah MD5

Langkah-langkah pembuatan message digest secara garis besar:

1. Penambahan bit-bit pengganjal (*padding bits*).
2. Penambahan nilai panjang pesan semula.
3. Inisialisasi penyangga (*buffer*) MD.
4. Pengolahan pesan dalam blok berukuran 512 bit.

3.2 Inisialisasi MD5

Pada MD-5 terdapat empat buah word 32 bit register yang berguna untuk menginisialisasi message digest pertama kali. Register-register ini diinisialisasikan dengan bilangan hexadesimal.

word A : 01 23 45 67

word B : 89 AB CD EF

word C : FE DC BA 98

word D : 76 54 32 10

Register-register ini biasa disebut dengan nama chain variable atau variabel rantai.

3.3 Proses Pesan Di Dalam Blok 16 Word

Pada MD-5 juga terdapat 4 (empat) buah fungsi nonlinear yang masing-masing digunakan pada tiap operasinya (satu fungsi untuk satu blok), yaitu:

$$F(X,Y,Z) = (X \dot{\cup} Y) \dot{\cup} ((\emptyset X) \dot{\cup} Z)$$

$$G(X,Y,Z) = (X \dot{\cup} Z) \dot{\cup} (Y \dot{\cup} (\emptyset Z))$$

$$H(X,Y,Z) = X \dot{\Delta} Y \dot{\Delta} Z$$

$$I(X,Y,Z) = Y \dot{\Delta} (X \dot{\cup} (\emptyset Z))$$

($\dot{\Delta}$ untuk XOR, $\dot{\cup}$ untuk AND, $\dot{\cup}$ untuk OR dan \emptyset untuk NOT).

Pada Gambar 1 dapat dilihat satu buah operasi dari MD-5 dengan operasi yang dipakai sebagai contoh adalah:

$$FF(a,b,c,d,Mj,s,ti) \text{ menunjukkan } a = b + ((a + F(b,c,d) + Mj + ti) \lll \lll)$$

$$FF(a,b,c,d,Mj,s,ti) \text{ menunjukkan } a = b + ((a + F(b,c,d) + Mj + ti) \lll \lll)$$

$$GG(a,b,c,d,Mj,s,ti) \text{ menunjukkan } a = b + ((a + G(b,c,d) + Mj + ti) \lll \lll)$$

$$HH(a,b,c,d,Mj,s,ti) \text{ menunjukkan } a = b + ((a + H(b,c,d) + Mj + ti) \lll \lll)$$

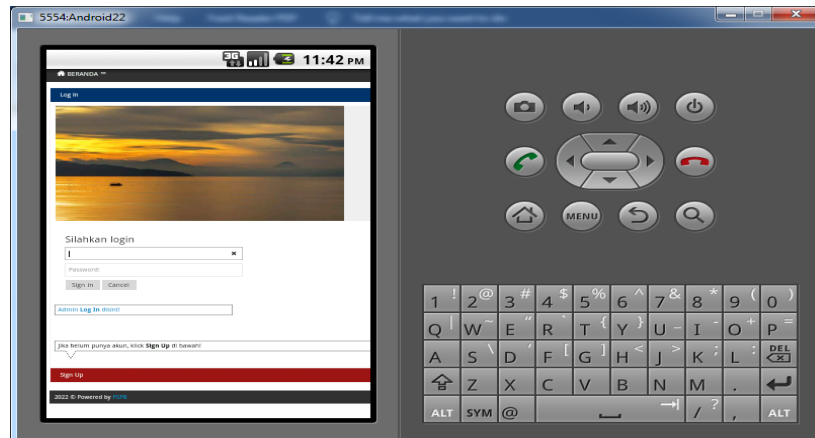
$$II(a,b,c,d,Mj,s,ti) \text{ menunjukkan } a = b + ((a + I(b,c,d) + Mj + ti) \lll \lll)$$

3.4 Implementasi Sistem

Berikut ini akan dijelaskan tampilan hasil dari aplikasi yang telah dibuat, yang digunakan untuk memperjelas tentang tampilan-tampilan yang ada pada perancangan aplikasi touring berbasis android. Sehingga hasil penerapannya sesuai dengan hasil program yang telah dirancang. Adapun tampilan yang ada pada tiap halaman *androidsite* dapat dilihat dibawah ini:

a. Tampilan login

Tampilan halaman ini berisikan tampilan awal dalam menjalankan perancangan aplikasi grup *touring* berbasis android yaitu berupa tampilan login, tampilan login dapat dilihat pada gambar dibawah ini :



Gambar 2 Tampilan Login

b. Tampilan Menu Utama

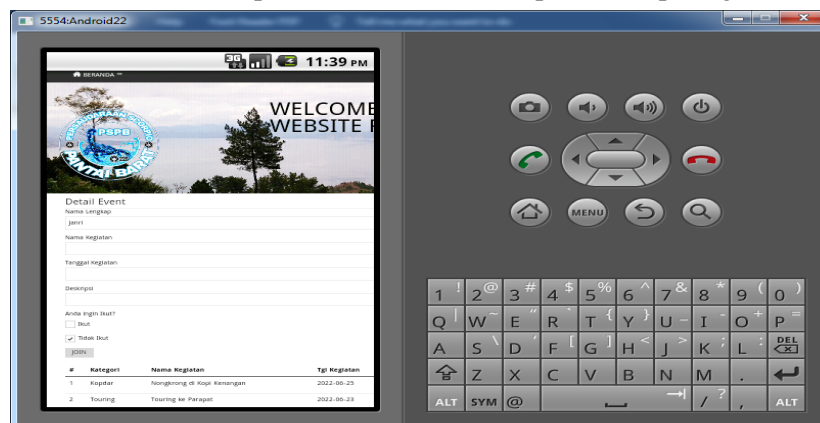
Tampilan halaman ini berisikan tampilan dalam menjalankan perancangan aplikasi grup *touring* berbasis android, tampilan menu utama dapat dilihat pada gambar dibawah ini :



Gambar 2 Tampilan Menu Utama

c. Tampilan Form Data Event

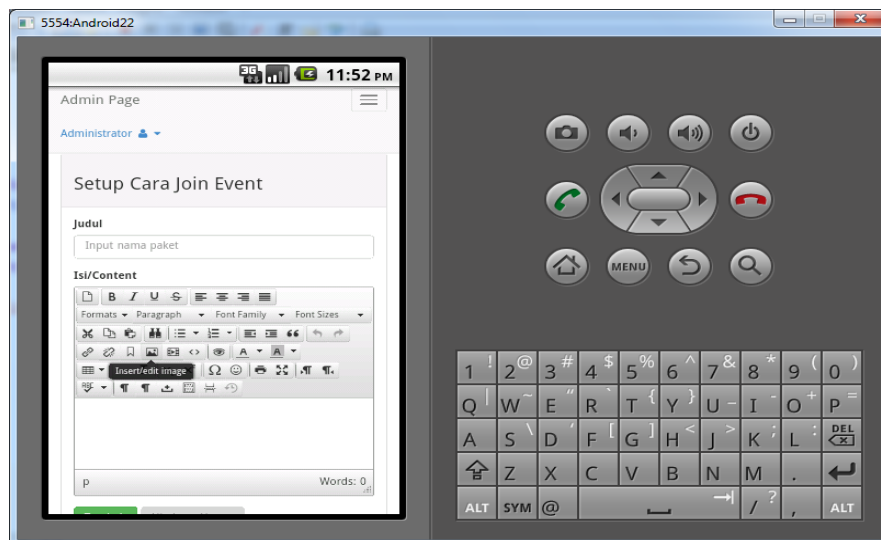
Tampilan halaman ini berisikan data *event* yang menjadi kegiatan untuk setiap aktifitas di dalam maupun diluar android, tampilan form data event dapat dilihat pada gambar dibawah ini:



Gambar 3 Tampilan Form Data Event

d. *Tampilan Form Event*

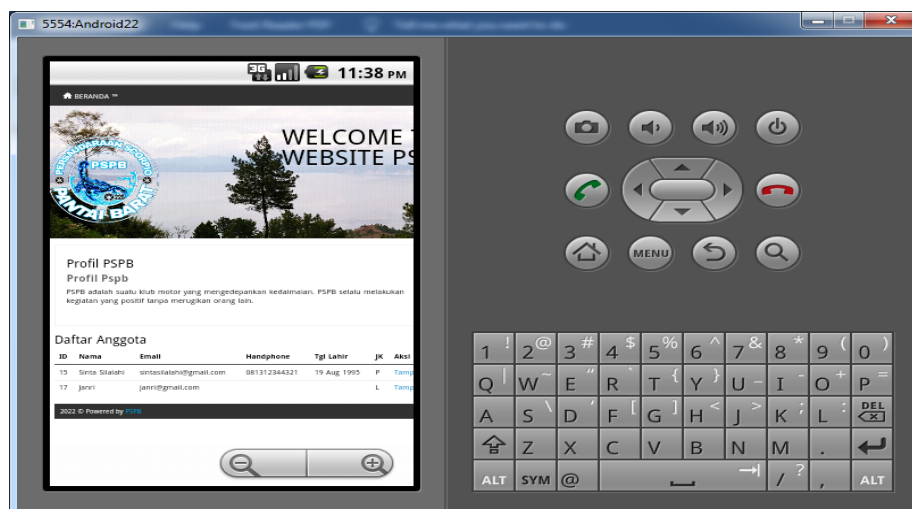
Tampilan halaman ini berisikan *form join event* dan cek *joint event* yang berfungsi untuk melihat daftar kegiatan *club* motor. Tampilan dapat dilihat pada gambar dibawah ini:



Gambar 4 Tampilan Form Event

e. *Tampilan Form Profil*

Tampilan halaman ini berisikan form profil anggota setelah login atau membuat akun baru, tampilan dapat dilihat pada gambar dibawah ini:



Gambar 5 Tampilan Form Profil

f. *Profil Anggota*

Tampilan ini berisikan anggota profil. Data ini didapat dari member yang melakukan registrasi hingga mejadi anggota club, tampilan dapat dilihat pada gambar dibawah ini:



Gambar 6 Tampilan Profil Anggota

g. Tampilan Form Identitas Member

Tampilan ini berisikan halaman identitas lengkap para member, identitas ini menjadi syarat sah untuk bisa menjadi member, selain itu data diri juga diperlukan guna kepentingan umum dan personal. Tampilan dapat dilihat pada gambar dibawah ini:

Gambar 7 Tampilan Form Identitas Member

h. Tampilan Form Inputan Member

Tampilan ini berfungsi sebagai inputan untuk menjadi member baru di *club* motor ini, *form* ini berisi dengan kebutuhan sistem akan biodata member seperti nama, ktp, alamat dan foto kendaraan. Tampilan dapat dilihat pada gambar dibawah ini:

Gambar 8 Tampilan Form Inputan Member

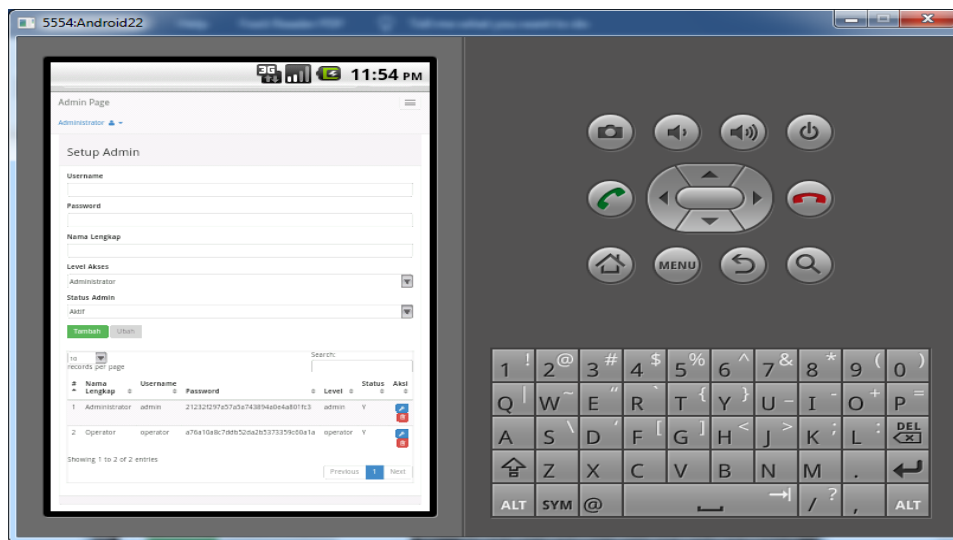
i. *Tampilan Form Login Admin*

Tampilan halaman ini berisikan login untuk admin sebagai pengolah data didalam sistem perlu diketahui, setiap data yang ada didalam *androidsite* ini adalah tugas dari admin, admin yang mengatur jadwal kegiatan didalam *event* dan rencana *touring club*. Tampilan dapat dilihat pada gambar dibawah ini:

Gambar 9 Tampilan Form Login Admin

j. *Tampilan Form Setting Admin*

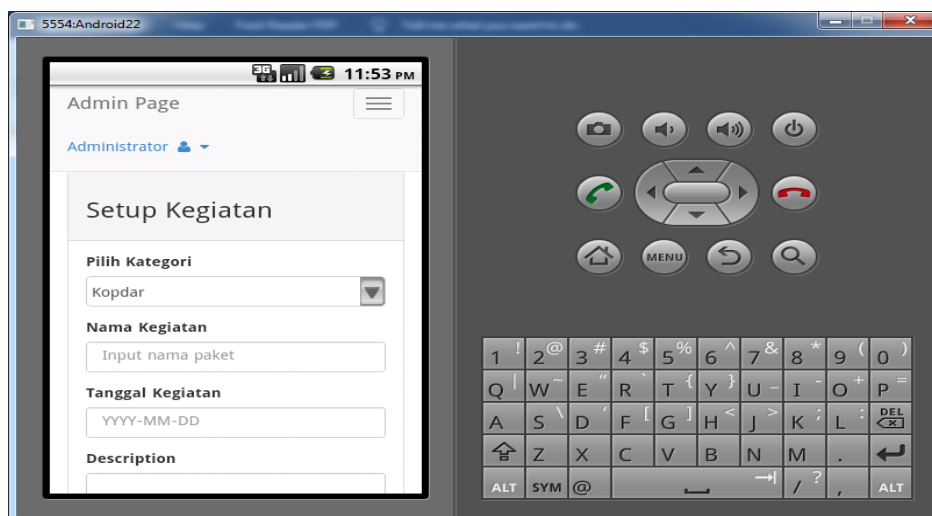
Tampilan halaman ini halaman admin yang berisikan *setting* tiap pengolahan didalam *androidsite* seperti mengatur kegiatan dan *event*, pengaturan anggota baru, tampilan dapat dilihat pada gambar dibawah ini:



Gambar 10 Tampilan Form Setting Admin

k. *Tampilan Form Setting Kegiatan*

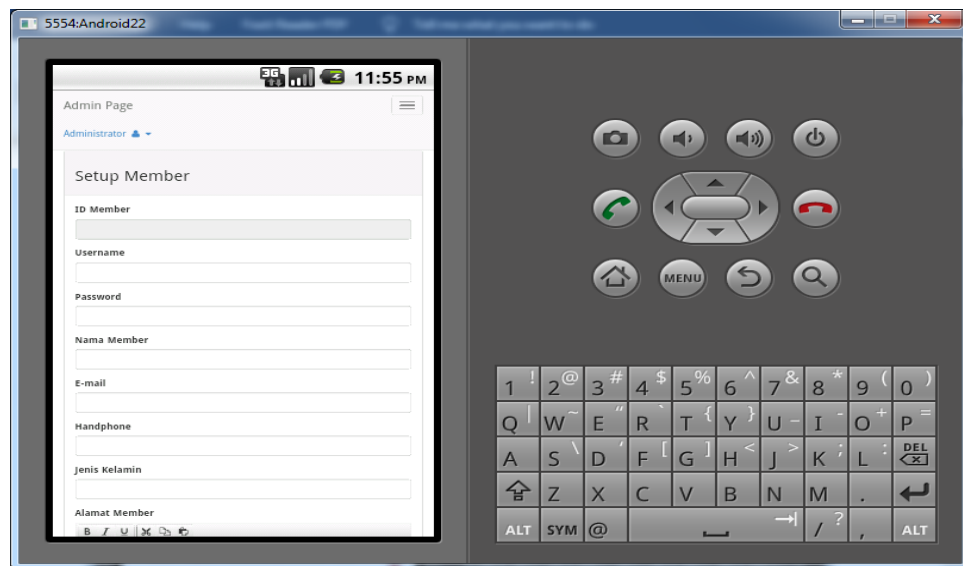
Tampilan halaman ini halaman admin yang berisikan *setting* kegiatan didalam *androidsite*, tampilan dapat dilihat pada gambar dibawah ini:



Gambar 11 Tampilan Form Setting Kegiatan

l. Tampilan Form Setting Setup Member

Tampilan halaman ini berisikan *setup* member, memungkinkan *admin* untuk memverifikasi *member* yang baru saja mendaftar masuk kepada *club* motor, tampilan dapat dilihat pada gambar dibawah ini:



Gambar 12 Tampilan Form Setting Setup Member

4. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian yang telah dilakukan maka penulis mengambil beberapa kesimpulan, diantaranya adalah sebagai berikut :

1. Dengan menerapkan metode MD5 pada *username* dan *password* berfungsi sebagai enkripsi menjaga keamanan akun pada anggota.
2. Berdasarkan pengujian yang telah dilakukan memperoleh aplikasi grup *touring* berbasis android menggunakan metode MD5 sebagai enkripsi *username* dan *password*.

DAFTAR PUSTAKA

- [1] P. M. Yusup, N. Komariah, N. Prahatmaja, and S. CMS, "Pemanfaatan Internet Untuk Penghidupan Di Kalangan Pemuda Pedesaan," *Baca J. Dokumentasi Dan Inf.*, vol. 40, no. 2, p. 217, 2019, doi: 10.14203/j.baca.v40i2.491.
- [2] K. YUSUF, "Penerapan Algoritma Md5 Sebagai Pengaman Akun Pada Aplikasi Web Emusrenbang Kota Binjai," *JTIK (Jurnal Tek. Inform. Kaputama)*, vol 4, no. 1, pp. 29-34, 2020, [Online]. Available: <https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/221>
- [3] Anam, M. K., & Anwar, R. (2020). Penerapan Aplikasi Pendukung Touring pada Komunitas Motor Berbasis Android. *Edumatic : Jurnal Pendidikan Informatika*, 4(1), 1–10. <https://doi.org/10.29408/edumatic.v4i1.1980>
- [4] Rahardi, M., & Aminuddin, A. (2021). Rancang Bangun Aplikasi Smart Touring Berbasis Android. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, 21(1), 159–168. <https://doi.org/10.30812/matrik.v21i1.1185>
- [5] Andriansah. (2021). Rancang Bangun Aplikasi Tours and Travel Berbasis Web. *Journal Speed – Sentra Penelitian Engineering Dan Edukasi*, Vol. 13 No. 1(1), 48–53. speed.web.id