

**QUICK RESPONSE CODE ABSENSI GURU
MENGUNAKAN *SECURE HASHING*
*ALGORITHM (SHA)***
(Study kasus SMP Negeri 4 lolayan)

Oleh
AGRIYANTO ASIKING
T3117147

SKRIPSI



**PROGRAM SARJANA
TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS ICHSAN GORONTALO
2021**

PENGESAHAN SKRIPSI

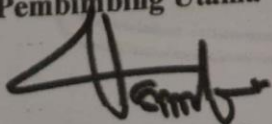
***QUICK RESPONSE CODE ABSENSI GURU
MENGUNAKAN SECURE HASHING
ALGORITHM (SHA)***
(Study kasus SMP Negeri 4 lolayan)

Oleh
AGRIYANTO ASIKING
T3117147

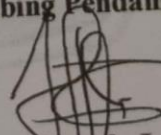
SKRIPSI

Untuk memenuhi salah satu syarat ujian guna memperoleh gelar Sarjana Progam
Studi Teknik Informatika, ini telah disetujui oleh Tim Pembimbing
Gorontalo,Desember 2021

Pembimbing Utama


Asmaul Husna, M.Kom
NIDN: 0911108602

Pembimbing Pendamping


Irma Surya Kumala I, M.Kom
NIDN: 0921128801

PERSETUJUAN SKRIPSI

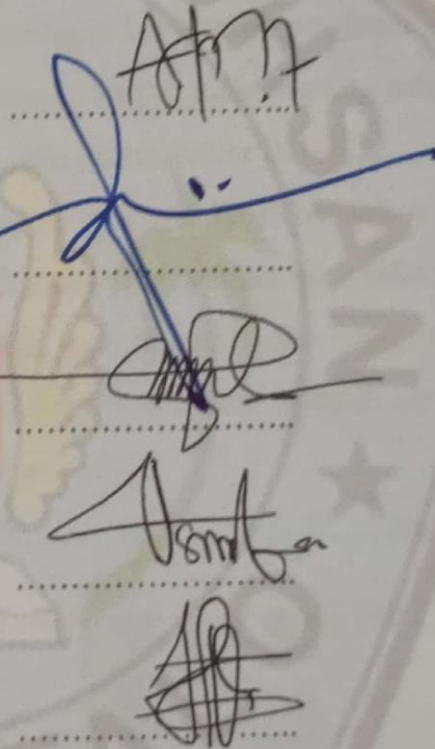
QUICK RESPONSE CODE ABSENSI GURU MENGUNAKAN SECURE HASHING ALGORITHM (SHA)

(Study kasus SMP Negeri 4 lolayan)

Oleh
AGRIYANTO ASIHING
T3117147

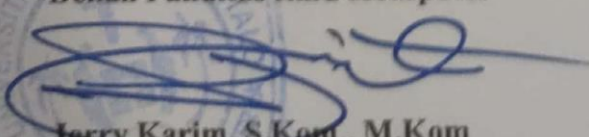
Diperiksa oleh Panitia Ujian Strata Satu (S1)
Universitas Ichsan Gorontalo

1. Ketua Penguji
Yasin Aril Mustofa, M.Kom
2. Anggota
Budy Santoso, S.Kom, M,Eng
3. Anggota
Yusrianto Malago, S.Kom., M.Kom
4. Anggota
Asmaul Husna N, M.Kom
5. Anggota
Irma Surya Kumala I, M.Kom

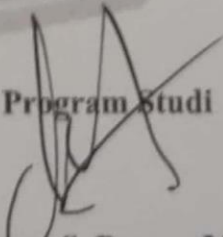


Mengetahui:

Dekan Fakultas Ilmu Komputer


Jerry Karim, S.Kom., M.Kom
NIDN.0918077302

Ketua Program Studi


Sudirman S. Panna, M.Kom
NIDN.0924038205

PERNYATAAN SKRIPSI

Dengan ini saya menyatakan bahwa:

1. Karya tulis (Skripsi) saya ini adalah asli dan belum pernah diajukan untuk mendapat gelar akademik (Sarjana) baik di Universitas Ichsan Gorontalo maupun di perguruan tinggi lainnya.
2. Karya tulis (Skripsi) saya ini adalah murni gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan dari Tim Pembimbing.
3. Dalam Karya tulis (Skripsi) saya ini tidak terdapat karya atau pendapat yang telah dipublikasikan orang lain, kecuali secara tertulis dicantumkan sebagai acuan/sitasi dalam naskah dan dicantumkan pula dalam daftar Pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidak benaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma-norma yang berlaku di Universitas Ichsan Gorontalo.

Goro:



2021

Agrivanto Asikang

T3117147

ABSTRACT

AGRIYANTO ASIKING. T3117147. THE IMPLEMENTATION OF SHA-256 CRYPTOGRAPHIC ALGORITHM FOR A QUICK RESPONSE CODE OF ATTENDANCE

The objective of this research is to implement the SHA-256 cryptographic algorithm for a Quick Response Code attendance. The encryption results from SHA-256 will be combined with the BCRYPT algorithm to avoid SHA-256 hash decoding attacks. The hash function is executed using the PHP programming language. The result shows that the Quick Response Code attendance with SHA-256 encryption has fulfilled the programming logic requirements, where $CC = V(G) = 2$ based on white-box testing. The system is free from component errors based on black-box testing, and the system can be used by SMP Negeri 1 Lolayan. This Quick Response Code attendance of teachers using the modified SHA-256 can be implemented.

Keywords: Quick Response Code, attendance, Secure Hash Algorithm

ABSTRAK

AGRIYANTO ASIKING. T3117147. IMPLEMENTASIKAN ALGORITMA KRIPTOGRAFI SHA-256 UNTUK PEMBUATAN *QUICK RESPONSE CODE* ABSENSI

Tujuan penelitian ini adalah mengimplementasikan algoritma kriptografi SHA-256 untuk pembuatan *Quick Response Code* absensi. Hasil enkripsi dari SHA-256 akan dikombinasi dengan algoritma BCRYPT untuk menghindari serangan decode hash SHA-256. Fungsi hash dijalankan dengan menggunakan bahasa pemrograman PHP. Hasil penelitian menunjukkan bahwa *Quick Response Code* absensi dengan enkripsi SHA-256 telah memenuhi syarat logika pemrograman, dimana $CC = V(G) = 2$ berdasarkan pengujian white-box. Sistem sudah bebas dari kesalahan komponen berdasarkan pengujian blackbox, dan sistemnya bisa digunakan oleh pihak SMP Negeri 1 Lolayan. *Quick Response Code* absensi guru dengan menggunakan SHA-256 yang telah dimodifikasi dapat diimplementasikan.

Kata kunci: *Quick Respon Code*, Absensi, *Secure Hash Algorithm*

KATA PENGANTAR

Segala Puji syukur penulis panjatkan kehadirat Allah SWT, karena atas berkat dan rahmat-Nya yang telah diberikan penulis dapat menyelesaikan Skripsi ini dengan judul ***“Quick Response Code Absensi Guru Menggunakan Secure Hashing Algorithm (SHA) (Study kasus SMP negeri 4 lolayan)”*** sesuai dengan harapan yang telah direncanakan oleh penulis. Penulis menyadari sepenuhnya bahwa skripsi ini tidak mungkin terwujud tanpa bantuan dan dorongan dari berbagai pihak, baik bantuan moril maupun materil. Untuk itu, dengan segala keikhlasan dan kerendahan hati, penulis mengucapkan banyak terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Muh. Ichsan Gaffar, S.E, M.Ak selaku Ketua Yayasan Pengembangan Ilmu Pengetahuan dan Teknologi (YPIPT) Ichsan Gorontalo.
2. Dr. Abd. Gaffar Latjoke, M.Si selaku Rektor universitas Ichsan Gorontalo.
3. Jorry Karim, S.kom., M.kom selaku Dekan Fakultas Ilmu Komputer.
4. Sudirman Melangi, M.Kom, selaku Wakil Dekan I Fakultas Ilmu Komputer.
5. Irma Surya Kumala Idris, M.Kom, selaku Wakil Dekan II Fakultas Ilmu Komputer sekaligus Dosen Pembimbing Pendamping, yang telah banyak membantu penyusunan skripsi.
6. Sudirman S Panna, M.Kom, selaku Ketua Program Studi Teknik Informatika.
7. Asmaul Husna, M.Kom selaku Dosen Pembimbing Utama, yang telah membimbing penulis selama mengerjakan skripsi ini.
8. Ucapan terima kasih Kepada Kedua orang tua saya yang tercinta dan keluarga penulis yang tercinta, atas segala kasih sayang, jerih payah dan doa restunya dalam membesarkan dan mendidik penulis.
9. Ucapan terima kasih Kepada rekan – rekan mahasiswa dan semua pihak yang ikut membantu dalam penyelesaian skripsi ini yang tak sempat sebutkan satu persatu.

Semoga Allah SWT, melimpahkan balasan atas jasa-jasa mereka kepada kami. Penulis memahami bahwa dalam penulisan skripsi penelitian ini masih memiliki

banyak kekurangan yang alangkah baiknya tidak menjadi penilaian yang buruk bagi penulis, namun menjadi pembelajaran penting serta pengalaman penting dalam penyusunan skripsi. Oleh karena itu, penulis sangat mengharapkan adanya kritik dan saran yang dapat memotivasi penulis dalam menyempurnakan skripsi ini. Akhirnya penulis mengharapkan manfaat dari apa yang telah dituangkan dalam skripsi ini, Aamiin.

Gorontalo, November 2021

Penulis

DAFTAR ISI

PERSETUJUAN SKRIPSI	Error! Bookmark not defined.
PENGESAHAN SKRIPSI	i
PERNYATAAN SKRIPSI.....	iii
ABSTRACT	iv
ABSTRAK	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Rumusan Masalah	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
BAB II LANDASAN TEORI	5
2.1 Tinjauan Studi	5
2.2 Tinjaun Pustaka	8
2.2.1 <i>Quick Response Code</i>	8
2.2.2 Pengertian Absensi.....	11
2.2.3 Pengertian Guru	11
2.2.4 <i>Secure Hash Algorithm</i> 256 (SHA-256)	12
2.2.5 Android	14

2.2.6	Web Service	16
2.2.7	Pemrograman Java dan <i>Android Studio IDE</i>	17
2.2.8	HTML, PHP, Dan MYSQL	18
2.2.9	<i>Unified Modelling Language (UML)</i>	20
2.2.10	Pengujian Sistem.....	25
2.3	Kerangka Pikir.....	29
BAB III METODE PENELITIAN.....		30
3.1	Objek Penelitian	30
3.2	Metode Penelitian.....	30
3.3	Pengumpulan Data	31
3.4	Pemodelan	32
BAB IV ANALISIS DAN PERANCANGAN		33
4.1	Jenis, Metode, Subjek dan Lokasi Penelitian	33
4.2	Pengumpulan Data	33
4.3	Dasar Prinsip SHA-256	33
4.4	Cara kerja SHA-256	34
4.5	Bcrypt	40
4.5.1	Salt	41
4.5.2	Cost.....	41
4.5.3	Proses Pengamanan Password Dengan Algoritma Bcrypt.....	42
4.6	Pembangunan Sistem	43
4.7	Activity Diagram Login	44
4.8	Activity Diagram Kelola Data Guru.....	45
4.9	Activity Diagram Buat QRCode	46
4.10	Activity Diagram Scan <i>Quick Response Code</i>	47

4.11	Sequence Diagram Login.....	48
4.12	Sequence Diagram Kelola Data Guru.....	48
4.13	Sequence Diagram Buat <i>Quick Response Code</i>	49
4.14	Sequence Diagram Scan <i>Quick Response Code</i>	49
4.15	Arsitektur Sistem	50
4.16	Interface Design.....	50
4.16.1	Mekanisme User.....	50
4.16.2	Mekanisme Navigasi Home	50
4.16.3	Mekanisme Login.....	51
4.16.4	Mekanisme Input Data Guru.....	52
4.16.5	Mekanisme Hapus dan Ubah Data Guru.....	53
4.16.6	Mekanisme Buat QRCode.....	53
4.16.7	Mekanisme Output	53
4.17	Hasil Pengujian Sistem	54
4.17.1	Pengujian White Box	54
4.17.2	FlowChart.....	55
4.17.3	Flowgraph Pengujian White Box	56
4.17.4	Perhitungan CC Pada Pengujian White Box.....	56
4.17.5	Perhitungan Basis Path Pada Pengujian White Box	57
4.17.6	Pengujian Black Box.....	57
BAB V HASIL DAN PEMBAHASAN.....		59
5.1	Pembahasan Sistem	59
5.1.1	Tampilan Login.....	59
5.1.2	Tampilan Halaman Utama	60
5.1.3	Tampilan Profil Admin	61

5.1.4	Tampilan Tambah Data Guru	61
5.1.5	Tampilan Buat <i>Quick Response Code</i>	62
5.1.6	Tampilan Daftar Guru	62
5.1.7	Tampilan Data QRCode	63
BAB VI KESIMPULAN DAN SARAN		67
6.1	Kesimpulan.....	67
6.2	Saran	67
DAFTAR PUSTAKA		68
LAMPIRAN		72

DAFTAR TABEL

Tabel 2.1. Penelitian Terkait	5
Tabel 2.2. Nilai Awal Variabel SHA-256.....	13
Tabel 2.3. Daftar Versi Android	14
Tabel 2.4. Simbol Use Case Diagram	21
Tabel 2.5. Simbol <i>Activity Diagram</i>	22
Tabel 2.6. Simbol <i>Sequence Diagram</i>	24
Tabel 4.1. Hasil Padding Pesan.....	34
Tabel 4.2. Hasil Parsing Pesan.....	35
Tabel 4.3. Hasil Message Schadule	36
Tabel 4.4. Konstanta SHA-256	37
Tabel 4.5. Nilai Putaran	39
Tabel 4.6. Mekanisme User	50
Tabel 4.7. Pseucode Proses Input QRCode.....	54
Tabel 4.8. Basis Path.....	57
Tabel 4.9. Tabel Pengujian <i>Blackbox</i> Admin.....	57
Tabel 4.10. Tabel Pengujian <i>Blackbox</i> Guru	58

DAFTAR GAMBAR

Gambar 2.1. Anatomi QR Code [13]	9
Gambar 2.2. Struktur QR Code [13]	10
Gambar 2.3. Skema <i>Web Service</i>	16
Gambar 2.4. Android Studio	17
Gambar 2.5. Notasi Diagrami Alir	26
Gambar 2.6. Diagram Alir prosedur Data	27
Gambar 2.7. Kerangka Pikir	29
Gambar 3.1. Langkah-langkah <i>R&D</i>	30
Gambar 3.2. Model Modifikasi SHA-256	32
Gambar 4.1. <i>Intermediate Hash Value In 1st Iteration</i>	37
Gambar 4.2. Sistem yang diusulkan	43
Gambar 4.3. Activity Diagram Login	44
Gambar 4.4. Activity Diagram Kelola Data Guru	45
Gambar 4.5. Activity Diagram Buat <i>Quick Response Code</i>	46
Gambar 4.6. Activity Diagram Scan <i>Quick Response Code</i>	47
Gambar 4.7. Sequence Diagram Login	48
Gambar 4.8. Sequence Diagram Kelola Data Guru	48
Gambar 4.9. Sequence Diagram Buat Quick Response Code	49
Gambar 4.10. Sequence Diagram Scan Quick Response Code	49
Gambar 4.11. Mekanisme Home Admin	50
Gambar 4.12. Mekanisme Navigasi Home Guru	51
Gambar 4.13. Mekanisme Login Admin	51
Gambar 4.14. Mekanisme Login Guru	52
Gambar 4.15. Mekanisme Input Data Guru	52
Gambar 4.16. Mekanisme Hapus dan Ubah Data Guru	53
Gambar 4.17. Mekanisme Buat QRCode	53
Gambar 4.18. Mekanisme Output	53
Gambar 4.19. Flowchart	55
Gambar 4.20. Flowgraph	56

Gambar 5.1. Tampilan Login Admin	59
Gambar 5.2. Tampilan Login Guru.....	59
Gambar 5.3. Tampilan Halaman Utama Admin	60
Gambar 5.4. Tampilan Halaman Utama Guru	60
Gambar 5.5. Tampilan Profil Admin	61
Gambar 5.6. Tampilan Tambah Data Guru.....	61
Gambar 5.7. Tampilan Buat Quick Response Code	62
Gambar 5.8. Tampilan Daftar Guru	62
Gambar 5.9. Tampilan Data Quick Response Code	63

BAB I

PENDAHULUAN

1.1 Latar Belakang

Absensi merupakan salah satu penunjang yang dapat mendukung atau memotivasi setiap kegiatan yang dilakukan di dalam dunia pendidikan di Indonesia [1]. Absensi memiliki peran penting dalam kehidupan sehari-hari terutama di lingkungan sekolah, universitas, pabrik, perkantoran, rumah sakit dan tempat lain yang membutuhkan Absensi [2]. Dengan adanya absensi, kedisiplinan setiap individu dapat diketahui untuk selanjutnya dapat dilakukan evaluasi kinerja sesuai dengan pekerjaan yang menjadi tugas dan tanggung jawab seseorang.

Absensi guru merupakan evaluasi awal untuk mengetahui hadir atau tidaknya seorang guru di Sekolah. Hal ini dilakukan agar dapat menjaga kedisiplinan guru dalam mengemban tanggung jawab sebagai pengajar. Kedisiplinan guru menjadi sangat berarti bagi keberhasilan seorang guru dalam mengajar dan kemajuan sekolah serta meningkatkan prestasi belajar siswa [3]. Sehingga dapat disimpulkan bahwa absensi guru dapat dijadikan sebagai tolak ukur awal dalam menilai bagaimana seorang guru disiplin terhadap waktu dan tanggung jawabnya untuk menghadiri jam kerja yang telah ditentukan oleh pihak Sekolah.

Pada Penelitian ini, penulis melakukan studi kasus di Sekolah Menengah Pertama (SMP) Negeri 4 Lolayan yang terletak di Desa Mopusi, Kecamatan Lolayan, Kabupaten Bolaang Mongondow. Sistem absensi guru yang diterapkan di Sekolah tersebut masih bersifat manual, yaitu guru datang mengisi buku absensi dengan menandatangani kolom absensi yang tersedia pada buku absen. Saat mengisi buku absen, guru menandatangani dan menuliskan jam kehadiran sehingga guru bebas menuliskan jam kehadiran sesuai keinginannya ataupun seorang guru dapat menitipkan tanda tangan absen. Hal ini bisa menimbulkan kecurangan dalam hal absensi guru. Adapun buku absen dan alat tulis yang digunakan sudah disiapkan lebih dulu, sehingga

semua guru menggunakan alat tersebut secara bergantian. Hal ini dikhawatirkan dapat meningkatkan potensi penyebaran virus COVID-19 yang masih menjadi pandemi hingga saat ini. Perlu diketahui bahwa potensi penyebaran virus COVID-19 dapat dicegah dengan menghindari kontak fisik atau penggunaan suatu benda umum yang disentuh oleh orang banyak.

Berdasarkan fenomena yang telah dijelaskan diatas maka penulis akan membuat aplikasi absensi dengan memanfaatkan teknologi antara *Quick Response Code* yang menggunakan *Secure Hash Algorithm* (SHA) dan *Smartphone Android* sehingga mengurangi kontak fisik atau penggunaan benda yang disentuh oleh orang banyak secara bergantian.

Quick Response Code atau *QR Code* merupakan hasil perkembangan teknologi pada *smartphone* yang berbentuk matrik 2 dimensi dengan pembacaan yang cepat dan kapasitas penyimpanan karakter yang lebih besar. *Quick Response Code* saat ini telah banyak digunakan di dunia industri, perdagangan, dan dunia Pendidikan [4]. *Quick Response Code* merupakan pengembangan dari barcode satu dimensi dan merupakan salah satu tipe dari barcode yang dapat dibaca dengan menggunakan kamera handphone [5]. *Quick Response Code* dapat diterapkan pada absensi guru karena mudah digunakan pada *smartphone android* namun memiliki keamanan yang tinggi karena dikombinasikan dengan *Secure Hash Algorithm* (SHA).

Secure Hash Algorithm (SHA) merupakan salah satu algoritma kriptografi yang digunakan untuk melakukan *encrypt* pesan atau karakter. Fungsi *hash* pada *Secure Hash Algorithm* (SHA) hanya bekerja satu arah, sehingga pesan atau karakter yang telah diubah menjadi pesan *digest* tidak dapat dikembalikan menjadi pesan atau karakter semula. Dua pesan atau karakter yang berbeda akan menghasilkan nilai hash yang berbeda pula [6]. Maka untuk menghindari pemalsuan *Quick Response Code* yang saat ini mudah dilakukan karena aplikasi *generating Quick Response Code* sudah tersedia pada *smartphone*, penulis tertarik untuk menggunakan *Secure Hash Algorithm* (SHA) pada *Quick Response Code* absensi guru agar *QR Code* absensi guru tidak dapat dipalsukan.

Pada penelitian ini penulis mengacu pada penelitian sebelumnya tentang penerapan *Quick Response Code* atau *QR Code* yang dilakukan oleh Eugenius Kau Suni dengan judul Penerapan Digital Signature Untuk Mengesahkan Proposal Hibah Dikti Menggunakan *Secure Hash Algorithm* [7], yaitu dengan kesimpulan bahwa sistem pengesahan dokumen proposal Hibah Dikti dengan digital signature menggunakan *secure hash alogrithm* ini telah diselesaikan dengan baik dan mampu memudahkan proses pengesahan Proposal Hibah Dikti yang sebelumnya dilakukan secara manual.

Adapun penelitian yang dilakukan oleh Adiat Pariddudin dengan judul Penerapan *Algoritma AES* pada *Quick Response Code* Untuk Keamanan Verifikasi Tiket [8], dengan kesimpulan bahwa penerapan *Algoritma Andvanced Encryption Standard* atau AES pada *Quick Response Code* (QR Code), sistem mampu menjaga keamanan data identitas tiket dari penjualan ulang tiket bekas pakai dan penggandaan tiket oleh orang yang tidak bertanggung jawab serta tersajinya informasi secara *real-time* mengenai tiket yang bisa di akses langsung oleh pelanggan dengan teknologi *Quick Response Code*.

Berdasarkan Latar belakang yang ada, maka penulis mengajukan penelitian dengan judul “***Quick Response Code Absensi Guru Menggunakan Secure Hashing Algorithm (SHA) (Study kasus SMP negeri 4 lolayan)***”. Dengan tujuan agar absensi guru di SMP Negeri 4 Lolayan mejadi lebih valid karena penggunaan *Quick Response Code* dan *Secure Hash Algorithm* (SHA) yang memiliki tingkat keamanan yang tinggi, serta meminimalisir kontak fisik atau penggunaan benda yang disentuh oleh orang banyak sehingga mengurangi potensi penyebaran virus COVID-19.

1.2 Identifikasi Masalah

Berdasarkan latar belakang dapat diidentifikasi masalah yaitu:

1. Proses absensi masih menggunakan buku dan alat tulis yang digunakan oleh orang banyak secara bergantian dan dapat ditulis sendiri oleh guru.

2. Perlunya membuat keamanan pada sistem absensi *Quick Response Code* yang dapat diterapkan pada *smartphone android*.

1.3 Rumusan Masalah

Adapun rumusan masalah yang dapat ditarik dari identifikasi masalah yaitu:

1. Bagaimana merancang aplikasi *Quick Response Code* Absensi Guru di SMP Negeri 4 Lolayan yang dapat melakukan *generate Quick Response Code* dan *Scan Quick Response Code*?
2. Bagaimana hasil penerapan *Secure Hash Algorithm* (SHA) pada *Quick Response Code* Absensi Guru di SMP Negeri 4 Lolayan?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini yaitu

1. Merancang aplikasi *Quick Response Code* Absensi Guru di SMP Negeri 4 Lolayan yang dapat melakukan *generate Quick Response Code* dan *Scan Quick Response Code*.
2. Mengetahui hasil penerapan *Secure Hash Algorithm* (SHA) pada *Quick Response Code* Absensi Guru di SMP Negeri 4 Lolayan.

1.5 Manfaat Penelitian

1. Manfaat Teoritis memberikan masukan bagi perkembangan ilmu pengetahuan dan teknologi, khususnya pada bidang ilmu komputer khususnya *Quick Response Code* Absensi Guru Menggunakan *Secure Hashing Algorithm* (SHA) (Study kasus SMP negeri 4 lolayan).
2. Manfaat Praktisi memberikan sumbangan pemikiran, karya, bahan pertimbangan, agar dapat menghasilkan sistem yang berkualitas yang dapat membantu pihak Sekolah dalam menerapkan *Quick Response Code* absensi Guru

BAB II

LANDASAN TEORI

2.1 Tinjauan Studi

Berikut penelitian yang terkait dengan penerapan *Quick Response Code* dan Fungsi *Hash* SHA yaitu:

Tabel 2.1. Penelitian Terkait

No	Peneliti	Judul	Tahun	Metode	Hasil
1	Ivan Wijaya, Dyah Erny Herwindiati, Janson Hendryli [9]	Smart Presensi Mengguna- kan <i>Quick Response Code</i> Dengan <i>Secure Hash Algorithm 2 (SHA-2)</i>	2021	Algoritma Kriptografi <i>Secure Hash Algorithm (SHA)</i>	Pada pengujian scanning <i>Quick Response Code</i> mendapatkan isi dari <i>Quick Response Code</i> yang dimiliki setiap mahasiswa akan berupa hasil fungsi <i>hash</i> SHA – 512 dari data mahasiswa, dan hal ini akan menjadikan setiap data mahasiswa akan terlindungi karena data mahasiswa hanya akan menampilkan datanya jika <i>Quick Response Code</i> mahasiswa tersebut dipindai oleh aplikasi mobile yang dimiliki oleh pengawas ujian.

No	Peneliti	Judul	Tahun	Metode	Hasil
2	Eugenius Kau Suni, Haidar Ilham Maulana [7].	Penerapan <i>Digital Signature</i> Untuk Mengesahan Proposal Hibah Dikti Mengguna- kan <i>Secure Hash Algorithm</i>	2020	Algoritma Kriptografi <i>Secure Hash Algorithm</i> (SHA)	Sistem yang dihasilkan ini untuk mengatasi masalah dan kendala pada proses pengesahan usulan Proposal Penelitian Hibah Dikti yang saat ini masih dikerjakan dengan cara konvensional. Penelitian ini menambah pengeta- huan tentang penggunaan <i>secure hash algorithm (SHA)</i> dalam pembuatan tanda tangan digital atau biasa disebut digital signature. Selanjutnya Implementasi sistem menambah pemahaman tentang pemanfaatan tanda tangan digital dalam meningkatkan efektivitas dan efisiensi pengesahan proposal Hibah Dikti
3	Adiat Pariddudin, Fatih Syauqi [8].	Penerapan Algoritma AES pada <i>Quick Response Code</i> Untuk	2018	Algoritma Kriptografi AES (<i>Advanced Encryption Standard</i>)	<i>Quick Response Code</i> sebagai pengganti kartu tiket yang dikerjakan oleh sistem dengan melakukan verifikasi dan me- nerapkan Algoritma AES.

No	Peneliti	Judul	Tahun	Metode	Hasil
		Kemanan Verifikasi Tiket			Penerapan <i>QRCode</i> pada sistem verifikasi kartu tiket tersebut yaitu untuk mengurangi resiko pengandaan tiket karena kode tiket terenkripsi dengan algoritma AES dan kode tiket akan diubah setiap 60 detik sehingga duplikasi tiket tidak bisa dilakukan.

Berdasarkan penelitian terkait diatas, penulis mengambil kesimpulan bahwa permasalahan pada *Quick Response Code* bukan terletak pada gambar yang dihasilkan saat melakukan generate *Quick Response Code* namun terletak pada karakter yang ada pada *Quick Response Code* itu sendiri. Penggunaan *Quick Response Code* hanyalah media untuk mempermudah user untuk mengidentifikasi suatu entitas atau produk. Namun saat ini, aplikasi *generate* maupun *reader Quick Response Code* mudah didapatkan secara gratis pada *Smartphone Android*. Misal seseorang dapat melihat isi dari *Quick Response Code* yang telah dibuat, Sehingga mereka dapat membuat *Quick Response Code* dengan meniru isi dari *Quick Response Code* yang telah dibaca sebelumnya. Berdasarkan permasalahan tersebut, maka ditemukan solusi yaitu penerapan algoritma kriptografi untuk melakukan enkripsi karakter yang ada pada *Quick Response Code*, sehingga ketika seseorang ingin menggandakan *Quick Response Code* dengan meniru isi dari *Quick Response Code*, maka *Quick Response Code* tersebut tidak dapat digunakan pada aplikasi yang telah dirancang dengan menerapkan fungsi Hash pada scanning *Quick Response Code*.

2.2 Tinjauan Pustaka

2.2.1 Quick Response Code

Quick Response Code [10] yaitu sebuah gambar kode berbentuk dua dimensi yang merupakan matrik. Perusahaan Jepang Denso-Wave mengembangkan kode ini pada tahun 1994 dengan tujuan untuk menyampaikan informasi secara cepat dan juga mendapat tanggapan secara cepat. Menurut Saeful [11] teknik *labeling Quick Response Code* merupakan teknik pemberian kode unik barang dengan menggunakan label *Quick Response Code*. JSIKA menerangkan bahwa “*Quick Response Code* adalah pengembangan II-2 *Barcode* yang sebelumnya berbentuk garis-garis yang ketebalannya berbeda-beda”. Adapun kelebihan *Quick Response Code* dibandingkan dengan barcode.

- a) Data tersandi yang dapat disimpan dalam kapasitas besar. Tipe data yang dapat disandikan oleh *Quick Response Code* ada berbagai macam yaitu seperti numeris, karakter, Kanji, Hiragana, simbol, biner, bahkan mampu menyandikan karakter dengan jumlah 7089 dalam satu simbol saja.
- b) *Quick Response Code* hanya membutuhkan sepersepuluh ruangan dari ruang yang dibutuhkan oleh barcode untuk menyandikan data.
- c) *Quick Response Code* dapat dibaca dari berbagai arah (360 derajat) dengan cepat sehingga memudahkan *scanning*.

2.2.1.1 Karakteristik Quick Response Code

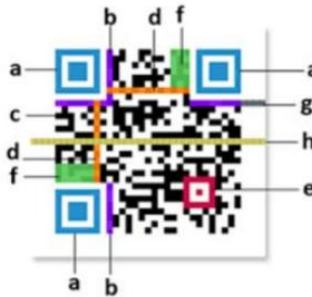
Google Menurut Setiadi [12], *Quick Response Code* memiliki karakteristik yaitu kemampuan dalam menampung jumlah data yang besar yaitu sebanyak 7089 karakter numerik maksimum data dapat tersimpan di dalamnya, kerapatan tinggi (100 kali lebih tinggi dari kode simbol linier) dan pembacaan kode dengan cepat. Adapun kelebihan *Quick Response Code* dalam proses kerja dan fungsi yaitu:

- 1) Pembacaan data dari segala arah (360 derajat).
- 2) Ketahanan terhadap penyimpanan symbol matrik 2 dimensi.

- 3) Fungsi pemulihan data dengan empat tingkatan koreksi eror (7%, 15%, 25%, dan 30%) di dalam mengendalikan kerusakan yang akibatnya kotor ataupun rusak.
- 4) Kemampuan encode karakter kanji dan kana.
- 5) Fungsi linking pada simbol yaitu kemampuan memecah kode menjadi beberapa bagian dengan maksimum pembagiannya 16 bagian.

2.2.1.2 Anatomi Quick Response Code

Berikut Gambar anatomi *Quick Response Code* [13]:



Gambar 2.1. Anatomi QR Code [13]

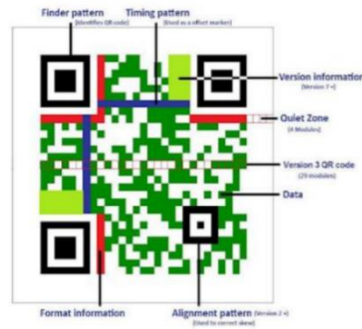
Adapun penjelasan anatomi *Quick Response Code* sesuai gambar diatas yaitu:

- a. Finder Pattern berfungsi untuk identifikasi letak *Quick Response Code*.
- b. Format Information berfungsi untuk informasi error correction level dan mask pattern.
- c. Data berfungsi untuk menyimpan data yang di kodekan.
- d. Timing Pattern merupakan pola yang berfungsi untuk identifikasi koordinat pusat *Quick Response Code*, berbentuk modul hitam.
- e. Alignment Pattern merupakan pola yang berfungsi memperbaiki penyimpangan *Quick Response Code* terutama distorsi non linier.
- f. Version Information adalah versi dari sebuah *Quick Response Code*.
- g. Quiet Zone merupakan bagian kosong.

- h. *Quick Response Code* Version adalah versi dari *Quick Response Code* yang digunakan.

2.2.1.3 Struktur *Quick Response Code*

Menurut Setiadi [12], *Quick Response Code* memiliki bagian-bagian struktur yang akan dijelaskan pada gambar berikut:



Gambar 2.2. Struktur QR Code [13]

Berikut ini merupakan penjelasan istilah-istilah yang berkenaan dengan gambar 2.2.

- 1) Finding pattern merupakan pola untuk mendeteksi posisi *Quick Response Code*.
- 2) Timing Pattern merupakan pola yang berfungsi untuk identifikasi koordinat pusat *Quick Response Code*, berbentuk modul hitam putih bergantian.
- 3) Version Information adalah versi dari sebuah *Quick Response Code*, versi terkecil adalah 1 (21 x 21) modul dan versi terbesar adalah 40 (117 x 117) modul.
- 4) Quiet Zone merupakan daerah kosong di bagian terluar *Quick Response Code* yang mempermudah mengenali pengenalan *Quick Response Code* oleh sensor CCD.
- 5) *Quick Response Code* Version adalah versi dari *Quick Response Code* yang digunakan pada contoh gambar, versi yang digunakan adalah versi 3(29 x 29) modul.

- 6) Data merupakan daerah tempat data tersimpan atau dikodekan.
- 7) *Alignment Pattern* merupakan pola yang berfungsi memperbaiki penyimpanan *Quick Response Code* terutama distorsi non linear.
- 8) *Format Information* berfungsi untuk informasi tentang error correction level dan mask pattern.

2.2.2 Pengertian Absensi

Absensi [14] adalah sebuah aktivitas pencatatan data untuk menyimpan data jumlah kehadiran Guru dan Siswa di Sekolah terhadap kegiatan yang membutuhkan informasi mengenai peserta tentu akan melakukan absensi salah satunya dalam kegiatan belajar mengajar. Absensi ini digunakan pada peserta didik dan juga pengajar. Salah satu manfaat absensi pada pihak masyarakat yaitu dalam perhitungan kemungkinan pegawai dalam kehadiran, sedangkan manfaat informasi absensi bagi pihak kepala sekolah antara lain untuk mengevaluasi pelayanan serta kualitas guru di Sekolah dan menjadi tolok ukur kedepannya agar kualitas dan pelayanan guru menjadi lebih optimal. Pengambilan data absensi ini sendiri dilakukan secara manual memiliki banyak kekurangan, seperti data yang tidak valid ketika data yang masuk salah.

2.2.3 Pengertian Guru

Menurut Hamid [15] Guru adalah salah satu komponen yang sangat penting dalam proses kegiatan belajar mengajar. Seorang guru memegang peran serta dalam usaha pembentukan sumber daya manusia yang berpotensi di bidang pembangunan. Semua guru berhak dan bertanggung jawab dalam kegiatan pembelajaran yang dilakukan di Sekolah maupun diluar Sekolah. Saat ini dapat kita temui bahwa Mata Pelajaran yang ditugaskan kepada guru berbeda dengan Program Studi yang dijalani saat dibangku kuliah sebelumnya. Hal ini mempengaruhi proses dan hasil pembelajaran oleh Guru kepada Murid. Oleh karena itu, menurut Hamid [15], guru profesional merupakan komponen yang sangat penting dalam bidang pendidikan dan pembelajaran.

Guru yang profesional memiliki tuntutan dalam bidangnya yaitu mampu mengajar dengan baik dengan menjadi sosok orang tua bagi murid-murid agar dapat mengatur murid-murid dengan baik. Selanjutnya mampu mengatur tahapan pembelajaran dengan baik dan rapi, apa yang akan diajarkan kepada murid harus dapat disusun dengan cermat terlebih dahulu agar mencapai hasil yang baik bagi Guru dan Murid yang diajar.

2.2.4 Secure Hash Algorithm256 (SHA-256)

SHA-2 adalah sebuah kriptografi fungsi hash yang dirancang oleh National Security Agency (NSA) dan dipublikasikan oleh National Institute of Standard and Technology (NIST) sebagai sebuah Federal Information Processing Standard (FIPS) oleh U.S. Ada empat algoritma untuk keamanan fungsi hash yaitu SHA-0, SHA-1, SHA-2, dan SHA-3. NIST memperbaharui SHA-2, dengan panjang output (256 atau 512- bit di atas 160-bit pada SHA-1) dan perbedaan-perbedaan pada SHA ini merupakan besar pesan yang ada pada proses komputasi [16].

SHA (Algoritma keamanan fungsi hash) merupakan algoritma enkripsi fungsi hash yang dapat digunakan untuk menghasilkan penggambaran konsolidasi dari sebuah data teks yang disebut sebuah proses pesan. SHA-256 dan SHA-512 adalah fungsi hash dengan kapasitas terbaru dengan panjang 32-bit dan 64-bit kata secara terpisah. Kedua fungsi hash ini dalam proses matematisnya menggunakan penjumlahan karakter yang berbeda dan ditambah dengan konstanta substansi. Meski demikian, struktur keduanya pada dasarnya tidak jauh berbeda, perbedaannya hanya terletak pada jumlah putaran saja [17].

Adapun proses atau tahapan pada algoritma SHA-256 adalah sebagai berikut [18]:

1. Message Padding

Pada tahap pertama ini, pesan berupa binary disisipkan dengan angka 1 dan ditambahkan bit-bit pengganjal, yakni angka 0 hingga panjang pesan kongruen

dengan 448 modulo 512. Panjang pesan asli ditambah sebagai angka biner 64 bit. Maka panjang pesan sekarang menjadi kelipatan 512 bit.

2. Parsing

Pada proses ini, pesan yang telah dipadding kemudian dibagi menjadi N buah blok 512 bit : $M(1)$, $M(2)$, ... $M(n)$

3. Message Expansion

Masing-masing blok 512 bit tadi dipecah menjadi 16 word 32 bit : $M0(i)$, $M1(i)$, ... $M15(i)$ Kemudian akan diperluas menjadi 64 word yang diberi label $W0$, $W1$,... $W63$.

4. Message Compression

Masing-masing dari 64 word yang diberi label $W0$, $W1$,... $W64$ tadi diproses dengan algoritma fungsi hash SHA-256. Dalam proses tersebut, inti utama dari algoritma SHA-256 adalah membuat 8 variabel yang diberikan nilai awal $L0$ - $L7$. Nilai awal tersebut adalah sebagai berikut:

Tabel 2.2. Nilai Awal Variabel SHA-256

L0	a	6A09E667	L4	E	510E527F
L1	b	BB67AE85	L5	F	9B05688C
L2	c	3C6EF372	L6	G	IF83D9AB
L3	d	A54FF53A	L7	H	5BE0CD19

- Kemudian dilakukan perhitungan sebanyak 64 kali putaran untuk setiap blok. Delapan variabel yang diberikan pada nilai awal berupa $L0$ sampai dengan $L7$ asumsikan menjadi nilai A, B, C, D, E, F, G , dan H nilainya terus berganti selama perputaran dengan rumus sebagai berikut:

$$T1 = h + s1 + CH + K[t] + W[t]$$

$$T2 = s0 + MAJ$$

$$h = g, g = f, f = e, e = d + T1, d = c, c = b, b = a, a = T1 + T2$$

Keterangan :

$$s0 = (a \ggg 2) \oplus (a \ggg 13) \oplus (a \ggg 22)$$

$$s1 = (e \ggg 6) \oplus (e \ggg 11) \oplus (e \ggg 25)$$

$$CH = (e \&f) \oplus ((\neg e)\&g))$$

$$MAJ = (a \&b) \oplus (a \&c) \oplus (b \&c)$$

Nilai akhir hash adalah sebagai berikut:

$$L0 = L0 + a$$

$$L1 = L1 + b$$

$$L2 = L2 + c$$

$$L3 = L3 + d$$

$$L4 = L4 + e$$

$$L5 = L5 + f$$

$$L6 = L6 + g$$

$$L7 = L7 + h$$

Maka, MD yang didapatkan adalah hasil akhir penjumlahan yang disusun secara memanjang [18].

2.2.5 Android

Android merupakan sistem operasi yang sangat populer digunakan pada perangkat cerdas atau *Smartphone*. Android pertama kali dikembangkan oleh perusahaan kecil di Silicon Valley yang bernama Android Inc. Pada tahun 2005, sistem operasi tersebut diambil alih oleh google dan menjadikan sistem operasi tersebut bersifat *open source* sehingga siapapun dapat menggunakannya dengan gratis, termasuk penggunaan kode sumber yang digunakan dalam pengembangan sistem operasi tersebut [19].

Sejak awal rilis versi android pertama yang tidak memiliki nama pada tanggal 23 september 2009 sampai saat ini, android terus berkembang dan versi baru telah bermunculan. Adapun versi android dapat dilihat pada table 1 berikut [19]:

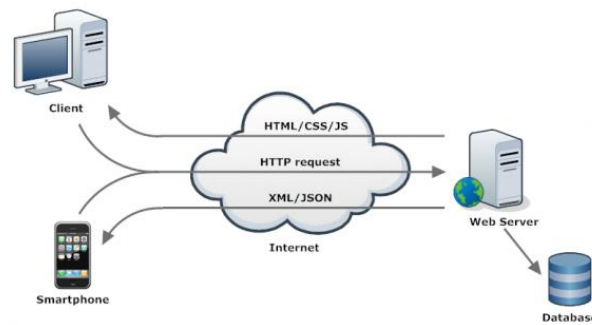
Tabel 2.3. Daftar Versi Android

No	Versi	Nama	Tanggal Rilis	Level API
1	1.0	N/A	23 September 2008	1
2	1.1	N/A	9 Februari 2009	2
3	1.5	Cupcake	27 April 2009	3
4	1.6	Donut	15 September 2009	4
5	2.0 - 2.1	Éclair	26 Oktober 2009	5 - 7
6	2.2 - 2.2.3	Froyo	20 Mei 2010	8
7	2.3 - 2.3.7	Gingerbread	6 Desember 2010	9 - 10
8	3.0 - 3.26	Honeycomb	22 Februari 2011	11 - 13
9	4.0 - 4.0.4	Ice Cream Sandwich	18 Oktober 2011	14 - 15
10	4.1 - 4.3.1	Jelly Bean	9 Juli 2012	16 - 18
11	4.4 - 4.4.4	Kitkat	31 Oktober 2013	19 - 20
12	5.0 - 5.1.1	Lollipop	12 November 2014	21 - 22
13	6.0 - 6.0.1	Marshmallow	5 Oktober 2015	23
14	7.0	Nougat	22 Agustus 2016	24
15	8.0	Oreo	21 Maret 2017	27
16	9.0	Pie	6 Agustus 2018	28
17	10.0	Q	13 Maret 2019	29

Penelitian ini akan di uji coba pada android versi *8.0 Oreo*. Uji coba program dilakukan di sistem operasi ini karena versi ini telah banyak pembaharuan fitur dan fungsi sistem operasi baik itu dari *software* dan *hardware* dari versi – versi sebelumnya. Pembaruan pada sistem operasi versi *8.0 Oreo* yaitu background limit sehingga meminimalisir penggunaan aplikasi di latar belakang, auto-fill salah satu fungsinya untuk menyimpan username saat diketik, picture-in-picture agar kita bisa menonton video sambil membuka aplikasi lainnya, dan beberapa fungsi lainnya. Dengan penggunaan sistem operasi versi *8.0 Ore* odapat menjadikan kinerja aplikasi menjadi lebih maksimal

2.2.6 Web Service

Web service merupakan kumpulan suatu layanan berbasis web dengan menggunakan jaringan protokol HTTP, layanan tersebut dapat diakses dan



dimanfaatkan oleh pengguna dengan bahasa pemrograman, arsitektur dan sistem operasi yang berbeda (interoperability). Web service harus bersifat stateless, sehingga dapat dibaca dan di akses multi-platform. Arsitektur pada web service dapat dibangun menggunakan Simple Object Access Protocol (SOAP) atau REpresentational State Transfer (REST), sementara service tersebut direpresentasikan dalam bentuk format teks, JSON atau XML. Pada umumnya formatnya menggunakan JSON dan XML [20]. Berikut gambar skema *web service*:

Gambar 2.3. Skema *Web Service*

Dari gambar di atas dapat kita lihat bahwa *web service* ternyata sangat berbeda dengan website. Perbedaan yang paling terlihat adalah website dibuat untuk memiliki tampilan (*user interface*) yang bagus, sedangkan *web service* tidak memiliki tampilan (*user interface*). Hal ini dikarenakan *web service* tidak dibuat untuk berinteraksi langsung dengan user. *Web service* hanya akan menyediakan *service* atau layanan. Layanan tersebut yang akan di gunakan atau dipanggil oleh aplikasi lainnya. Dengan demikian yang akan menjadi interface adalah aplikasi yang memanggil bukan *web service* itu sendiri.

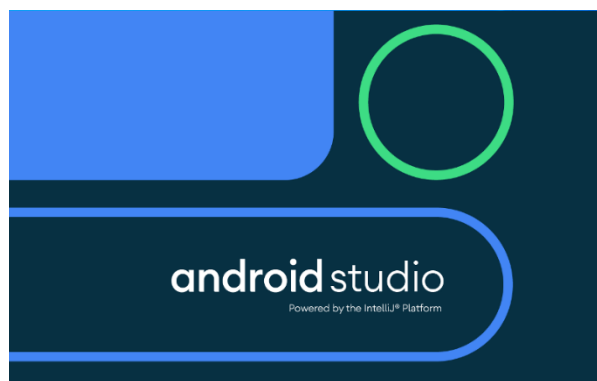
2.2.7 Pemrograman Java dan *Android Studio IDE*

2.2.7.1 Pemrograman Java

JAVA adalah bahasa pemrograman yang dapat dijalankan di berbagai komputer termasuk telepon genggam (*Cellular*). Bahasa ini awalnya dibuat oleh James Gosling saat masih bergabung di *Sun Microsystems* saat ini merupakan bagian dari *Oracle* dan dirilis tahun 1995. Bahasa ini banyak mengadopsi sintaksis yang terdapat pada C dan C++ namun dengan sintaksis model objek yang lebih sederhana serta dukungan rutin-rutin aras bawah yang minimal [21]. Karena *framework* android ditulis dengan bahasa pemrograman java, maka untuk dapat merancang aplikasi berbasis android kita wajib untuk mengetahui bahasa pemrograman java terlebih dahulu.

2.2.7.2 *Android Studio IDE (Integrated Development Environment)*

Android studio adalah *platform IDE (Integrated Development Enviroment)* resmi untuk pengembangan aplikasi *android* dan bersifat *open source* atau gratis. Peluncuran android studio diumumkan oleh google pada 16 mei 2013 pada event *Google I/O Conference* untuk tahun 2013. *Android studio* menggantikan *eclipse* sebagai IDE resmi untuk mengembangkan aplikasi android [22].



Gambar 2.4. Android Studio

Beberapa fitur yang didukung oleh android studio adalah:

1. Berbasis *Gradle*.
2. *Android-spesifik refactoring* dan perbaikan yang cepat.

3. *Tool Lint* untuk menangkap kinerja, kegunaan, versi kompatibilitas dan masalah lainnya.
4. *ProGuard* dan *app-signature*.
5. *Wizard* untuk *design* dan membuat komponen-komponen umum Sebuah *layout editor* yang memungkinkan untuk *drag-and-drop* komponen UI, pratinjau *layout* pada beberapa konfigurasi layar, dan banyak lagi.
6. *Built-in* dukungan untuk *Google Cloud platform*, sehingga mudah untuk mengintegrasikan *Google Cloud Messaging* dan *App Engine* sebagai komponen *server-side*.

2.2.8 HTML, PHP, Dan MYSQL

2.2.8.1 HTML

HTML merupakan singkatan dari *HyperText Markup Language*. Disebut *hypertext* karena didalam script HTML kita bisa membuat teks menjadi *link* yang dapat berpindah dari halaman satu ke halaman lainnya dengan meng-klik teks tersebut. Teks yang ber-*link* inilah yang dinamakan *hypertext* [23]. Selanjutnya disebut *markup language* karena *script html* menggunakan tanda (dalam bahasa inggris disebut *mark*) untuk menandai bagian-bagian dari teks agar teks itu memiliki tampilan/ fungsi tertentu.

2.2.8.2 PHP

PHP berasal dari kata *Hypertext Preprocessor*, yaitu Bahasa pemrograman universal untuk penanganan pembuatan dan pengembangan sebuah situs web dan bisa digunakan bersamaan dengan HTML. PHP sebagai sekumpulan skrip atau Bahasa program memiliki fungsi utama yaitu mampu mengumpulkan dan mengevaluasi hasil survei atau bentuk apapun ke server database dan pada tahap selanjutnya akan menciptakan efek beruntun PHP ini berupa Tindakan dari skrip lain yang akan melakukan komunikasi dengan *database*, mengumpulkan dan mengelompokkan informasi, kemudian menampilkannya pada saat ada tamu *website* memerlukannya (menampilkan informasi sesuai permintaan user) [24].

Bahasa pemrograman PHP merupakan bahasa pemrograman untuk membuat website yang bersifat server-side scripting. PHP bersifat dinamis. PHP dapat dijalankan pada berbagai macam sistem operasi seperti Windows, Linux, dan Mac Os. Selain Apache, PHP juga mendukung beberapa web server lain, seperti Microsoft ISS, Caudium, dan PWS. PHP dapat memanfaatkan database untuk menghasilkan halaman web yang dinamis [25].

Dapat disimpulkan bahwa PHP sebuah bahasa scriping yang ditempelkan dengan HTML (*Hyper Text Markup Language*) dan ditempatkan dalam server lalu diproses di server, yang mampu mendukung fasilitas data base dan bisa berjalan di berbagai sistem informasi

2.2.8.3 MYSQL

Pada perkembangannya, *MYSQL* disebut juga SQL yang merupakan singkatan dari Structured Query Language. SQL merupakan bahasa terstruktur yang khusus digunakan untuk mengolah database. SQL pertama kali didefinisikan oleh American National Standards Institute (ANSI) pada tahun 1986. *MYSQL* adalah sebuah sistem manajemen database yang bersifat open source [25].

MYSQL merupakan sistem manajemen database yang bersifat relational. Artinya, data yang dikelola dalam database yang akan diletakkan pada beberapa tabel yang terpisah sehingga manipulasi data akan jauh lebih cepat. *MYSQL* dapat digunakan untuk mengelola database mulai dari yang kecil sampai dengan yang sangat besar [25].

SQL juga dapat diartikan sebagai antar muka standar untuk sistem manajemen relasional, termasuk sistem yang beroperasi pada komputer pribadi. SQL memungkinkan seorang pengguna untuk mengetahui dimana lokasinya, atau bagaimana informasi tersebut disusun. SQL lebih mudah digunakan dibandingkan dengan bahasa pemrograman, tetapi rumit dibandingkan software lembar kerja dan pengolah data. Sebuah pernyataan SQL yang sederhana dapat menghasilkan set permintaan untuk informasi yang tersimpan pada komputer yang berbeda diberbagai lokasi yang tersebar, sehingga membutuhkan waktu dan sumber daya komputasi yang

banyak. SQLinte dapat digunakan untuk ivestigasi interaktif, atau pembuatan laporan ad hoc atau disisipkan dalam program aplikasi [25]

2.2.9 Unified Modelling Language (UML)

Unified Modelling Language (UML) merupakan satu kumpulan konvensi pemodelan yang digunakan untuk menentukan atau menggambarkan sebuah sistem software yang terkait dengan objek. UML adalah sebuah Bahasa pemodelan yang telah menjadi standar dalam industry software untuk visualisasi, merancang, dan mendokumentasikan sistem perangkat lunak. Bahasa pemodelan UML lebih cocok untuk pembuatan perangkat lunka dalam Bahasa pemrograman berorientasi objek (C++, java, VB.Net), namun demikian tetap dapat digunakan pada Bahasa pemrograman prosedural [26].

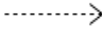
Pemodelan menggunakan Unified Modelling Language merupakan metode pemodelan berorientasi objek dan berbasis visual. Karenanya pemodelan menggunakan UML merupakan pemodelan objek yang fokus pada pendefinisian struktur statis dan model sistem informasi yang dinamis dari pada mendefinisikan data dan model proses yang tujuannya adalah pengembangan tradisional. UML menawarkan diagram yang dikelompokkan menjadi 5 perspektif berbeda untuk memodelkan suatu sistem seperti satu set blueprint yang digunakan untuk membangun sebuah rumah. Berikut ini penjelasan mengenai berbagai diagram UML serta tujuannya [26].

1. Use Case View

Use case view dapat dipresentasikan dengan urutan yang sederhana, dan akan mudah dipahami oleh para konsumen. Use case view adalah layanan atau juga fungsi yang ada pada sistem untuk para penggunanya [26]. Sedangkan untuk menggambarkan behavior dari sistem disebut dengan *Use Case Diagram*. *Use case Diagram* adalah gambaran efek fungsionalitas yang diharapkan oleh sistem. Komponen ini pastinya sangat membantu ketika sedang menyusun kebutuhan pada sebuah sistem, kemudian mengkomunikasikan rancangan aplikasi tersebut pada konsumen, dan juga merancang

test case untuk berbagai *fiture* yang ada di sistem [26]. Adapun konsep utama Use Case View digambarkan sebagai berikut [26]:

Tabel 2.4. Simbol Use Case Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		<i>Actor</i>	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan <i>use case</i> .
2		<i>Dependency</i>	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri (<i>independent</i>) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (<i>independent</i>).
3		<i>Generalization</i>	Hubungan dimana objek anak (<i>descendent</i>) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (<i>ancestor</i>).
4		<i>Include</i>	Menspesifikasikan bahwa <i>use case</i> sumber secara <i>eksplisit</i> .
5		<i>Extend</i>	Menspesifikasikan bahwa <i>use case</i> target memperluas perilaku dari <i>use case</i> sumber pada suatu titik yang diberikan.
6		<i>Association</i>	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		<i>System</i>	Menspesifikasikan paket yang menampilkan sistem secara terbatas.

NO	GAMBAR	NAMA	KETERANGAN
8		<i>Use Case</i>	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor
9		<i>Collaboration</i>	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan perilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).
10		<i>Note</i>	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

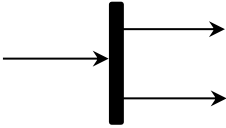
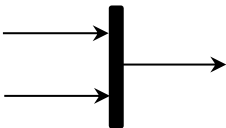
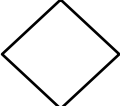
2. Activity View

Diagram aktivitas menunjukkan aliran *control prosedural* antara dua atau lebih banyak objek kelas saat memproses suatu kegiatan. Diagram aktivitas dapat berupa model yang digunakan untuk memodelkan proses bisnis tingkat yang lebih tinggi pada tingkat unit bisnis, atau untuk memodelkan tindakan kelas internal tingkat rendah. Untuk dapat membangun *activity diagram* yang baik, berikut proses yang unggul untuk membangun *activity diagram* [26]:

1. Tambahkan poin awal dan akhir pada sebuah *use case*
2. Tambahkan sebuah kegiatan untuk tiap langkah utama pada *use case* (atau tiap langkah utama setiap pelaku yang menginisialisasi)
3. Tambahkan transisi dari setiap kegiatan lain, poin keputusan, atau poin akhir
4. Tambahkan bar sinkronisasi dimana kegiatan dilakukan secara *parallel*.

Tabel 2.5. Simbol *Activity Diagram*

Simbol	Keterangan
	<i>Start Point</i>

Simbol	Keterangan
	<i>End Point</i>
	<i>Activities</i>
	<i>Fork (Percabangan)</i>
	<i>Join (Penggabungan)</i>
	<i>Decision</i>

Sumber: Kusnadi [26].

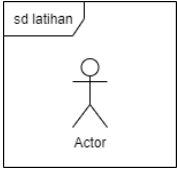
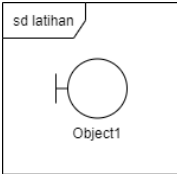
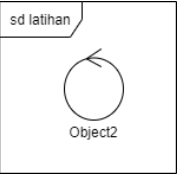
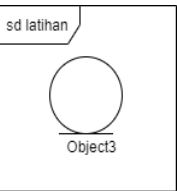
3. Interaction View

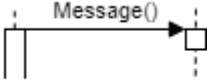
Fokus diagram interaksi adalah pada komunikasi antar garis hidup dalam berbagai format yaitu: pemanggilan meted, pengiriman sinyal, pembentukan instance, penghapusan objek, dan sebagainya, kesemuanya disebut pesan. Suatu pesan menspesifikasikan jenis komusikasi, pengirim dan penerimanya. Pesan yang sering digunakan biasanya berbentuk pemanggilan suatu metode antra dua objek. Jika pesan mengindikasikan suatu pemanggilan metode dalam sintaks pesan. Parameter-parameter itu harus salah satu dari:

1. Atribut dari objek pengiriman

2. Konstanta
3. Nilai simbolis
4. Parameter eksplisit dari penutup interaksi
5. Atribut kelas pemilik penutup interaksi [26].

Tabel 2.6. Simbol *Sequence Diagram*

Simbol	Keterangan
Aktor 	Menggambarkan orang yang sedang berinteraksi dengan sistem
Boundary Class 	Menggambarkan sebuah penggambaran dari form
Control Class 	Menggambarkan penghubung antara <i>boundary</i> dengan <i>table</i>
Entity Class 	Menggambarkan hubungan kegiatan yang akan dilakukan

Simbol	Keterangan
<i>A focus of & a life line</i> 	Menggambarkan tempat mulai dan berakhirnya sebuah <i>message</i>
<i>Message</i> 	menggambarkan pengiriman pesan

Sumber: Kusnadi [26].

2.2.10 Pengujian Sistem

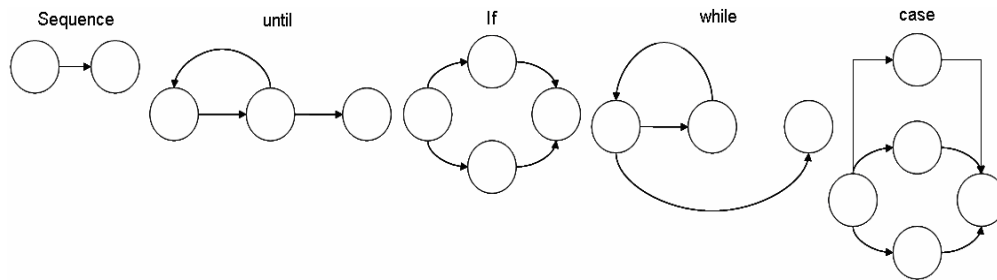
2.2.10.1 WhiteBox

Metode *White box* ini adalah pengujian perangkat lunak pada tingkat alur kode program, apakah masukan dan keluaran yang sesuai dengan spesifikasi yang dibutuhkan [27].

Pengujian *whitebox* memiliki beberapa komponen yaitu sebagai berikut:

a. Uji Coba Basis *Path*

Basis *Path* adalah suatu jalur unik yang melintasi alur program dan tidak diperbolehkan terjadinya perulangan lintasan yang sama. Pada metode pengujian basic path mengharuskan menghitung kompleksitas logis dari alur program dan menggunakan ukuran sebagai petunjuk untuk mendefinisikan jumlah jalur eksekusi [28].



Gambar 2.5. Notasi Diagram Alir

Lingkaran atau disebut juga *node*, merupakan gambaran satu atau lebih dari perintah prosedural. Urutan proses dan keputusan bisa dipetakan dalam satu node. Tanda panah atau disebut juga dengan *edge*, merupakan gambaran arus kontrol. Setiap *node* yang ada harus terhubung ke *node* lainnya.

b. Cyclomatic Complexity

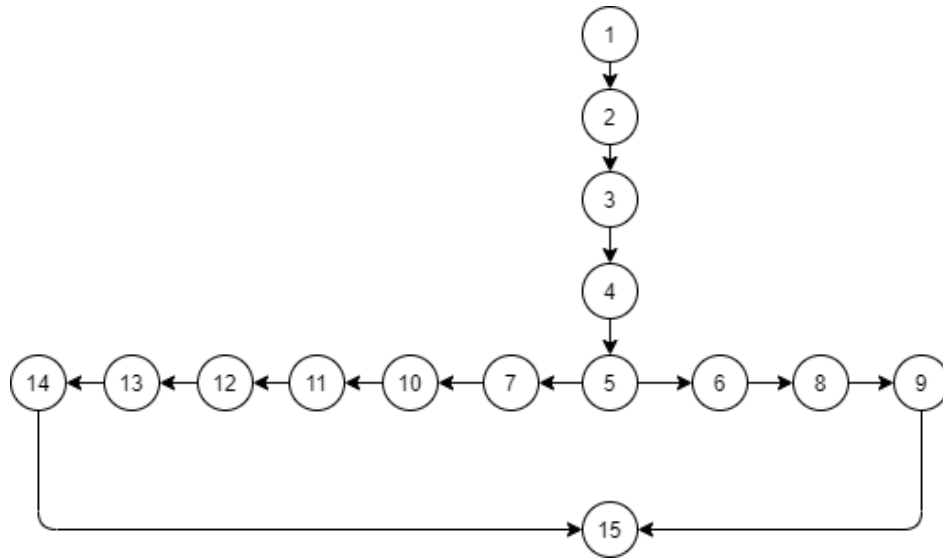
Cyclomatic complexity yaitu salah satu matrik yang cukup terkenal yang mana metric ini menghitung control flow dari suatu modul. Apabila kompleksitas semakin tinggi maka akan modul tersebut akan semakin sulit untuk diuji dan dirawat. Untuk menghitung cyclomatic complexity bisa dilakukan dengan dua cara yaitu yang pertama menghitung berdasarkan banyaknya nodes dan edge yang dirumuskan pada Persamaan. Kedua dengan cara menghitung node percabangan (predicate node) yang dirumuskan pada Persamaan.

c. Melakukan Test Case

Metode uji coba basis *path* juga dapat diterapkan pada perancangan prosedural rinci atau program sumber. Prosedur rata-rata pada bagian berikut akan digunakan sebagai contoh dalam pembuatan *test case*.

Langkah-langkah pembuatan *test case*

- a) Dengan mempergunakan perancangan prosedural atau program sumber sebagai dasar, digambarkan diagram alirnya.



Gambar 2.6. Diagram Alir prosedur Data

Sumber: Subagia (2020)

- b) Tentukan *cyclomatic complexity* (CC) untuk diagram alir:

Dari gambar 2.2.5, Subagia menyimpulkan sebagai berikut [29];

$$V(G) = 2 \text{ region}$$

$$V(G) = 15 \text{ edge} - 15 \text{ node} + 2 = 2$$

$$V(G) = 1 \text{ predicate node} + 1 = 2$$

- c) Tentukan *independent path* pada *flowgraph*

Dari hasil perhitungan CC terdapat 2 *independent path*, yaitu :

Path 1 : 1-2-3-4-5-6-8-9-15

Path 2 : 1-2-3-4-5-7-10-11-12-13-14-15

- d) Buat *test case* yang akan mengerjakan masing-masing path pada basis set. Data yang dipilih harus tepat sehingga setiap kondisi dari *predicate node* dikerjakan semua.

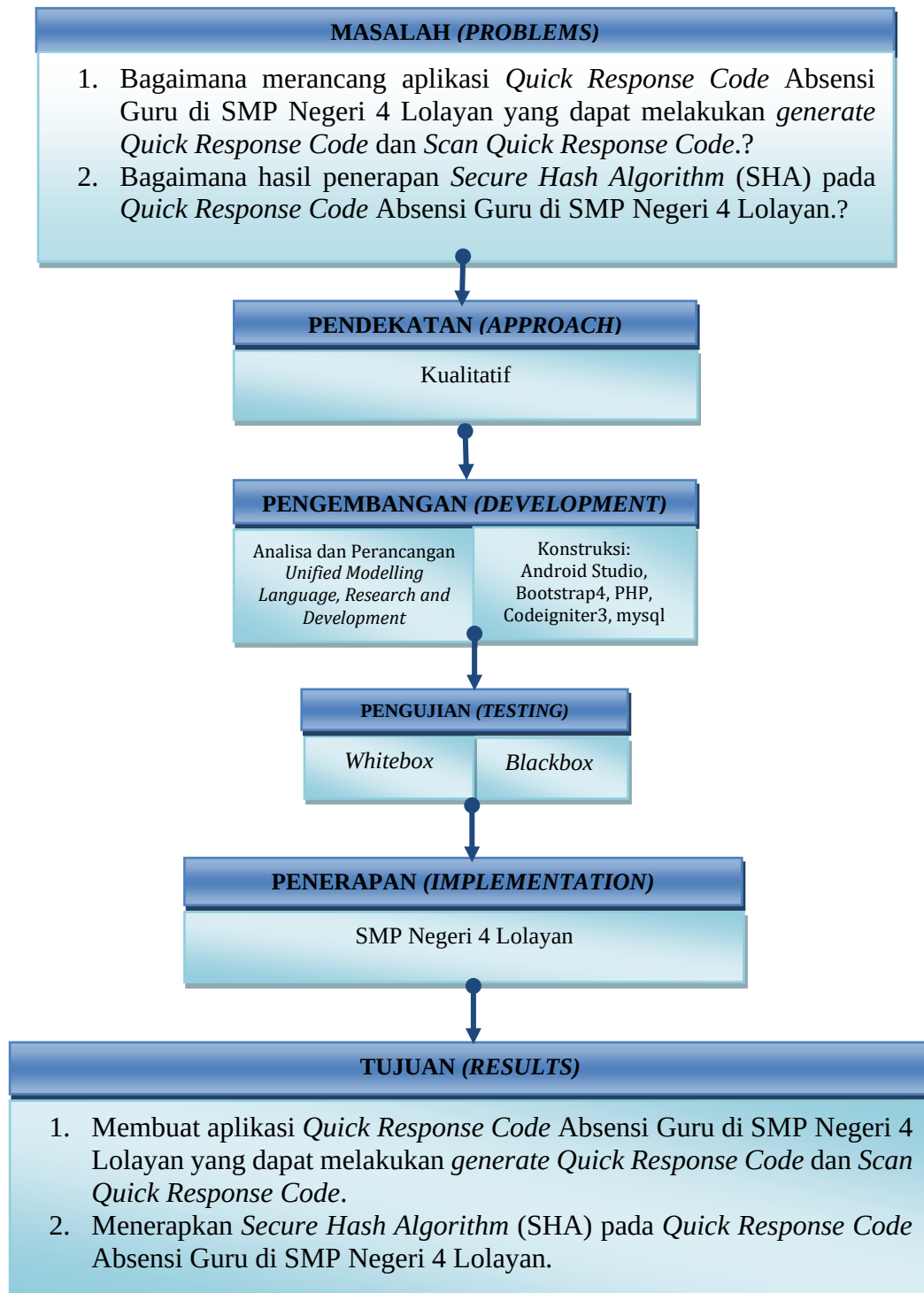
2.2.10.2 BlackBox

Metode ujicoba *black box* merupakan pengujian yang berfokus pada spesifikasi fungsional dari perangkat lunak, tester dapat mendefinisikan kumpulan kondisi input dan melakukan pengetesan pada spesifikasi fungsional program [30]. Ujicoba *black box* bukan merupakan alternatif dari ujicoba *white box*, tetapi merupakan pendekatan yang melengkapi untuk menemukan kesalahan lainnya, selain menggunakan metode *white box*. Ujicoba *blackbox* merupakan pendekatan yang melengkapi untuk menemukan kesalahan lainnya dan untuk menemukan kesalahan dalam beberapa kategori, diantaranya :

1. Fungsi-fungsi yang salah atau hilang
2. Kesalahans *interface*
3. Kesalahan dalam struktur data atau akses *database* eksternal
4. Kesalahan performa
5. kesalahan inisialisasi dan terminasi

Tidak seperti metode *whitebox* yang dilaksanakan diawal proses, ujicoba *blackbox* diaplikasikan di beberapa tahapan berikutnya. Karena ujicoba *blackbox* dengan

2.3 Kerangka Pikir



Gambar 2.7. Kerangka Pikir

BAB III

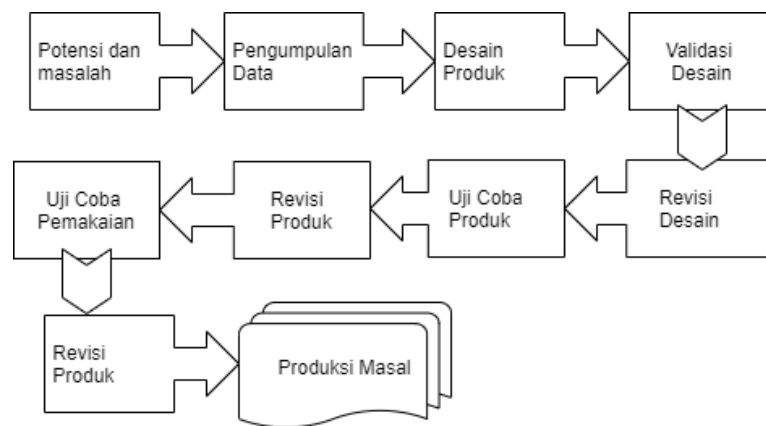
METODE PENELITIAN

3.1 Objek Penelitian

Adapun objek penelitian sesuai dengan pembahasan yang telah dijelaskan pada latar belakang yaitu implementasi SHA-256 untuk keamanan QRCode pada absensi Guru di SMP Negeri 1 Lolayan.

3.2 Metode Penelitian

Penelitian ini menggunakan metode *Research and Development* atau yang dikenal dengan metode Penelitian dan Pengembangan. Metode ini didefinisikan sebagai metode penelitian yang digunakan untuk menghasilkan produk tertentu dan menguji keefektifan produk tersebut. Menurut Saputro [31], *Metode Research and Development* adalah metode penelitian yang menghasilkan sebuah produk dalam bidang keahlian tertentu, yang diikuti produk sampingan tertentu serta memiliki efektifitas dari sebuah produk tersebut.



Gambar 3.1. Langkah-langkah R&D.

Metode *Research and Development* digunakan peneliti untuk pembuatan aplikasi *Quick Response Code* Absensi Guru Menggunakan *Secure Hashing Algorithm* (SHA).

Subjek penelitian ini adalah *Quick Response Code* pada objek Absensi Guru di SMP Negeri 4 Lolayan.

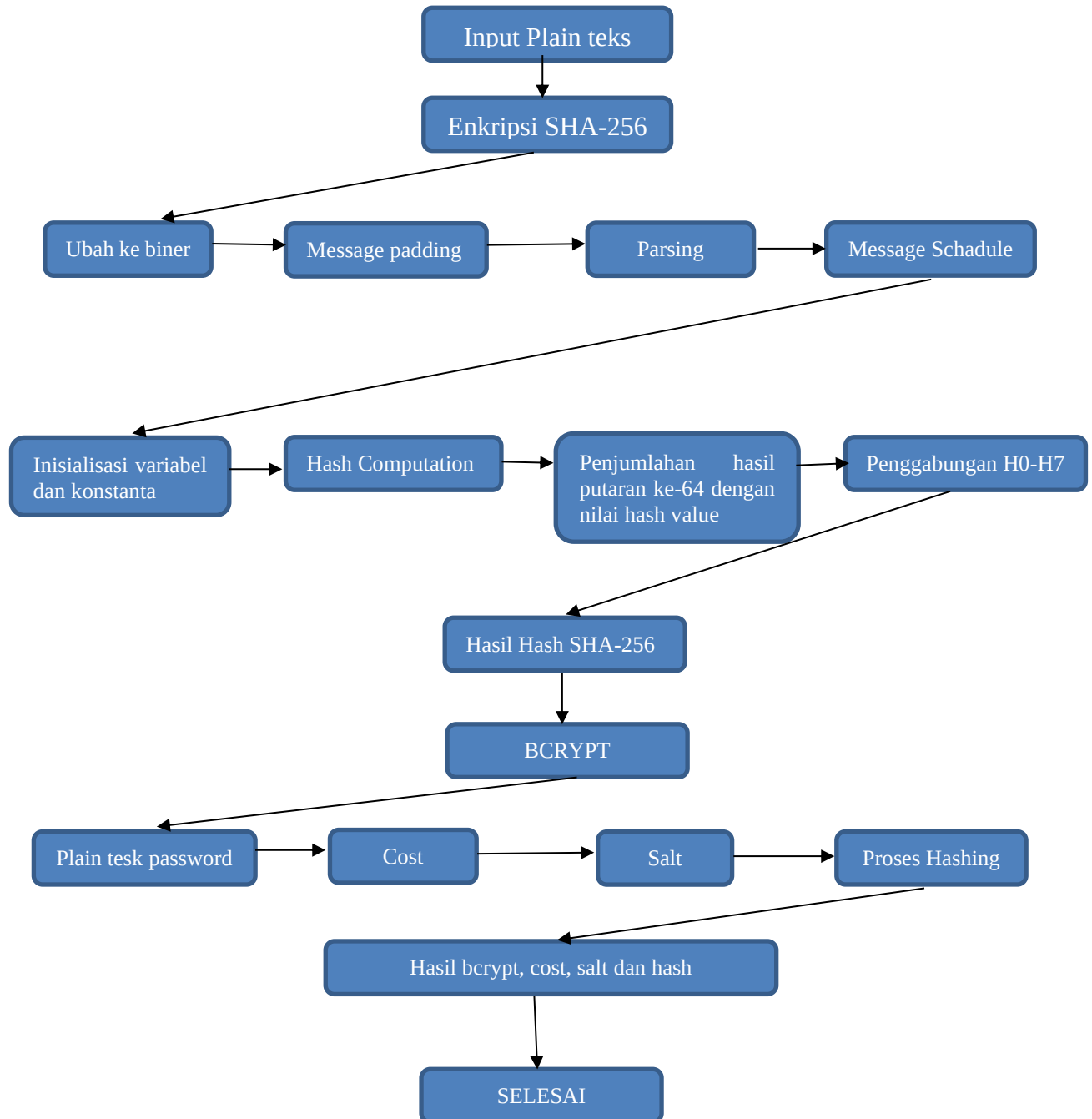
3.3 Pengumpulan Data

Adapun pengumpulan data dilakukan dengan dua teknik yaitu wawancara dan studi literatur. Data yang dikumpulkan dalam penelitian yaitu data primer dan sekunder.

- a. Data Primer dalam penelitian ini berupa data Guru SMP Negeri 4 Lolayan, data absensi Guru dan data umum lainnya. data ini diperlukan guna mendapatkan gambaran kepada peneliti dalam melakukan perancangan alur sistem nantinya.
- b. Data sekunder yang digunakan dalam penelitian yaitu penulis mengumpulkan data-data dan referensi yang dibutuhkan untuk menyempurnakan penulis proposal ini, contohnya yaitu referensi buku dan jurnal tentang penerapan *Quick Response Code* dan algoritma kriptografi SHA-256.

3.4 Pemodelan

Model yang diusulkan bisa dilihat pada gambar berikut ini.



Gambar 3.2. Model Modifikasi SHA-256

BAB IV

ANALISIS DAN PERANCANGAN

4.1 Jenis, Metode, Subjek dan Lokasi Penelitian

Berdasarkan dari tingkat penerapannya, maka jenis penelitian ini merupakan penelitian terapan. Sedangkan berdasarkan tujuannya, maka penelitian ini merupakan penelitian eksperimen. Dilihat dari jenis informasi yang diolah, bahwa penelitian ini merupakan penelitian Kualitatif.

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode *Research and Development*. Subjek penelitian ini adalah *Secure Hashing Algorith*m (SHA). Waktu dan lokasi penelitian di mulai dari bulan September 2021 sampai dengan Desember 2021 yang berlokasi di SMP negeri 4 Lolayan Kabupaten Bolaang Mongondow.

4.2 Pengumpulan Data

Tahapan awal pengembangan sistem ini yaitu komunikasi dan pengumpulan data. Komunikasi dan pengumpulan data pada penelitian ini yaitu mengumpulkan data yang diperoleh dari hasil wawancara langsung dengan pihak SMP Negeri 4 Lolayan. Data yang dibutuhkan dalam penelitian ini adalah data guru, data sampel absensi, dan informasi tentang sistem absensi yang diterapkan saat ini. Data ini dibutuhkan untuk analisis kebutuhan sistem.

4.3 Dasar Prinsip SHA-256

pembuatan *message-digest* didasarkan pada pesan dengan panjang maksimum 2^{64} bit. Menggunakan *message-schedule* yang terdiri dari:

- 64 elemen *word* 32-bit
- 8 buah variabel 32-bit
- Variabel penyimpan nilai hash 8 buah *word* 32-bit.

Hasil akhir didapat message-digest sepanjang 256bit.

4.4 Cara kerja SHA-256

mengubah pesan masukan ke dalam *message digest* 256 bit. Berdasarkan secure hashsing signature standard, pesan masukan yang panjangnya lebih pendek dari 2^{64} bit, harus dioperasikan oleh 512 bit dalam kelompok dan menjadi sebuah message diggest 256-bit.

Pada tahap ini sebuah plainteks dienkripsi dengan SHA-256 menggunakan bahasa PHP, setelah itu hasil hash SHA-256 akan diamankan dengan algoritma bcrypt. Plainteks yang dibuat, misalnya: 735 Berikut tahapan hash SHA-256 dengan plainteks 735:

- 1) Pesan diubah menjadi angka biner

7 = 00000111

3 = 00000011

5 = 00000101

Maka pesan, M = 00000111 00000011 00000101

Diketahui panjang pesan: l = 24 bit

- 2) *Message Padding*

Padding pesan dilakukan dengan cara menambahkan bit 1 dan sisanya adalah bit 0 hingga pesan sepanjang 512 bit. Untuk mencari jumlah nol yang ditambahkan (k) digunakan rumus berikut:

$$l + 1 + k = 448 \text{ mod } 512$$

$$k = 448 - 25 \text{ mod } 512$$

$$24 + 1 + k = 448 \text{ mod } 512$$

$$k = 423$$

Karena k = 423 maka banyaknya bit 0 yang akan ditambahkan adalah sebanyak 423 bit. Setelah itu ditambahkan jumlah panjang pesan pada akhir pesan yang dipadding sebanyak 8 bit dengan nilai l = 24 = 00011000.

Tabel 4.1. Hasil Padding Pesan

00000111	00000011	00000101	10000000	00000000	00000000	00000000	00000000
----------	----------	----------	----------	----------	----------	----------	----------

00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00011000

3) Parsing

Pesan yang telah dipadding akan menghasilkan blok pesan 512 bit $M(0)$, $M(1)$,... $M(n-1)$. Namun dalam kasus ini hanya menghasilkan satu blok 512 bit yaitu $M(0)$. Selanjutnya adalah membagi setiap blok 512 bit menjadi 16 buah word 32 bit sebagai berikut:

Tabel 4.2. Hasil Parsing Pesan

$M_0^{(0)}$	0000	0111	0000	0011	0000	0101	1000	0000
$M_0^{(1)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(2)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(3)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(4)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(5)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(6)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(7)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(8)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(9)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(10)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(11)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(12)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(13)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(14)}$	0000	0000	0000	0000	0000	0000	0000	0000
$M_0^{(15)}$	0000	0000	0000	0000	0000	0000	0001	1000

4) *Message Schedule*

Tahap selanjutnya yaitu masing-masing 16 word diatas diperluas menjadi 64 buah 32 bit word sebagai berikut:

Tabel 4.3. Hasil Message Schedule

W_0	07030580	W_{16}	00000000	W_{32}	00000000	W_{48}	00000000
W_1	00000000	W_{17}	00000000	W_{33}	00000000	W_{49}	00000000
W_2	00000000	W_{18}	00000000	W_{34}	00000000	W_{50}	00000000
W_3	00000000	W_{19}	00000000	W_{35}	00000000	W_{51}	00000000
W_4	00000000	W_{20}	00000000	W_{36}	00000000	W_{52}	00000000
W_5	00000000	W_{21}	00000000	W_{37}	00000000	W_{53}	00000000
W_6	00000000	W_{22}	00000000	W_{38}	00000000	W_{54}	00000000
W_7	00000000	W_{23}	00000000	W_{39}	00000000	W_{55}	00000000
W_8	00000000	W_{24}	00000000	W_{40}	00000000	W_{56}	00000000
W_9	00000000	W_{25}	00000000	W_{41}	00000000	W_{57}	00000000
W_{10}	00000000	W_{26}	00000000	W_{42}	00000000	W_{58}	00000000
W_{11}	00000000	W_{27}	00000000	W_{43}	00000000	W_{59}	00000000
W_{12}	00000000	W_{28}	00000000	W_{44}	00000000	W_{60}	00000000
W_{13}	00000000	W_{29}	00000000	W_{45}	00000000	W_{61}	00000000
W_{14}	00000000	W_{30}	00000000	W_{46}	00000000	W_{62}	00000000
W_{15}	00000018	W_{31}	00000000	W_{47}	00000000	W_{63}	00000000

5) *Inisialisasi Variabel dan Konstanta*

Variabel awal pada fungsi hash SHA-256 adalah sebagai berikut:

$$a = H_0(0) = 6A09E667$$

$$b = H_0(1) = BB67AE85$$

$$c = H_0(2) = 3C6EF372$$

$$d = H_0(3) = A54FF53A$$

$$e = H_0(4) = 510E527F$$

$$f = H_0(5) = 9B05688C$$

$$g = H_0(6) = 1F83D9AB$$

$$h = H_0(7) = 5BE0CD19$$

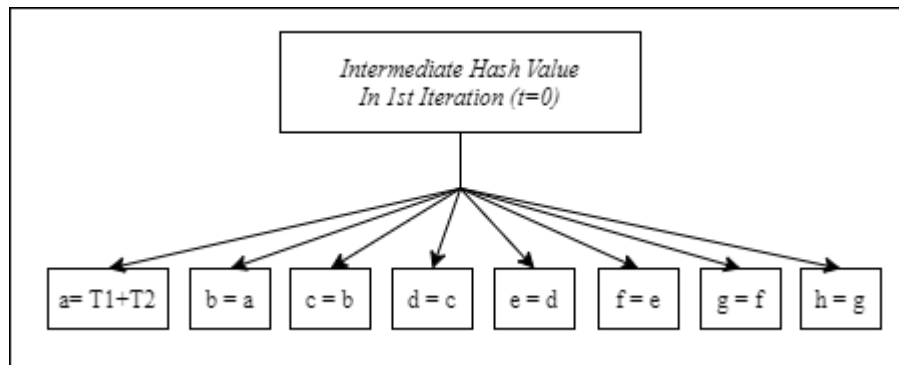
Nilai konstanta pada fungsi hash SHA-256 ($K_0\{256\}$, $K_1\{256\}$,.... $K_{63}\{256\}$) adalah sebagai berikut:

Tabel 4.4. Konstanta SHA-256

428A2F98	71374491	B5C0FBCF	E9B5DBA5	3956C25B	59F111F1	923F82A4	AB1C5ED5
D807AA98	12835B01	243185BE	550C7DC3	72BE5D74	80DEB1FE	9BDC06A7	C19BF174
E49B69C1	EFBE4786	0FC19DC6	240CA1CC	2DE92C6F	4A7484AA	5CB0A9DC	76F988DA
983E5152	A831C66D	B00327C8	BF597FC7	C6E00BF3	D5A79147	06CA6351	14292967
27B70A85	2E1B2138	4D2C6DFC	53380D13	650A7354	766A0ABB	81C2C92E	92722C85
A2BFE8A1	A81A664B	C24B8B70	C76C51A3	D192E819	D6990624	F40E3585	106AA070
19A4C116	1E376C08	2748774C	34B0BCB5	391C0CB3	4ED8AA4A	5B9CCA4F	682E6FF3
748F82EE	78A5636F	84C87814	8CC70208	90BEFFFA	A4506CEB	BEF9A3F7	C67178F2

6) Hash Computation

Dalam proses ini dilakukan perhitungan nilai a sampai nilai h sebanyak 64 kali putaran. Adapun bentuk perhitungannya adalah sebagai berikut:



Gambar 4.1. Intermediate Hash Value In 1st Iteration

Mencari nilai T1 dengan rumus: $T1 = h + S1(e) + ch(e, f, g) + kt + wt$

Dimana, h = nilai h pada iterasi sebelumnya

$$S1(e) = (e \ggg 6) \oplus (e \ggg 11) \oplus (e \ggg 25)$$

$$Ch(e, f, g) = (e \& f) \oplus ((\neg e) \& g)$$

Kt = Nilai Konstanta

Wt = Nilai W pada Message Schedule

Semua angka hexadesimal de konversikan ke biner lalu lakukan pergeseran dan penjumlahan sesuai rumus

Maka nilai T1 dapat dihitung seperti berikut:

$$h = 5BE0CD19$$

$$\begin{aligned} Si(e) &= (01010001000011100101001001111111 \text{ putar kanan 6 kali}) \oplus \\ &(01010001000011100101001001111111 \text{ putar kanan 11 kali}) \oplus \\ &(01010001000011100101001001111111 \text{ putar kanan 25 kali}) \end{aligned}$$

$$\begin{aligned} Si(e) &= 11111101010001000011100101001001(xor) \\ &01001111111010100010000111001010(xor) \\ &10000111001010010011111110101000 \end{aligned}$$

$$Si(e) = 001101011100001110010011100101011$$

$$Si(e) = 3587272B$$

$$\begin{aligned} ch(e, f, g) &= 01010001000011100101001001111111(\text{and}) \\ &10011011000001010110100010001100(xor)(\text{Not}1010111011110001101011011000 \\ &0000)(\text{and}) 00011111100000111101100110101011 \end{aligned}$$

$$ch(e, f, g) = 00001110100000011000100110000000$$

$$\begin{aligned} T1 &= 01011011111000001100110100011001(+) \\ &001101011100001110010011100101011(+)+00001110100000011000100110000000(\\ &+) 1000010100010100010111110011000 (+) 1110000000110000010110000000 \end{aligned}$$

$$T1 = 11110011111000111000000111110100$$

$$T1 = F3E381F4$$

Selanjutnya rumus untuk mencari nilai T2 adalah sebagai berikut:

$$T2 = S0(a) + Maj(a, b, c)$$

$$\text{Dimana, } S0(a) = (a \ggg 2) \oplus (a \ggg 13) \oplus (a \ggg 22)$$

$$Maj(a, b, c) = (a \& b) \oplus (a \& c) \oplus (b \& c)$$

Maka nilai T2 dapat dihitung seperti berikut:

$S0(a) = (11011010100000100111100110011001 \text{ putar kanan } 2 \text{ kali}) \text{ xor}$
 $(00110011001110110101000001001111 \text{ putar kanan } 13 \text{ kali}) \text{ xor}$
 $(00100111100110011001110110101000 \text{ putar kanan } 22 \text{ kali})$

$S0(a) = 11001110001000001011010001111110$

$S0(a) = CE20B47E$

$Maj(a, b, c) = (11001110001000001011010001111110(\&)$
 $10111011011001111010111010000101)(\text{xor})(1100111000100000101101000111111$
 $0\&)00111100011011101111001101110010)(\text{xor})$
 $(10111011011001111010111010000101(\&)00111100011011101111001101110010)$

$Maj(a, b, c) = 111010011011111110011001100100$

$Maj(a, b, c) = 3A6FE667$

$T2 = 11001110001000001011010001111110(+)111010011011111110011001100100$

$T2 = 100000001001101011100101$

$T2 = 08909AE5$

Setelah nilai T1 dan T2 ditemukan, maka nilai a adalah sebagai berikut:

$a = T1 + T2$

$a = 11110011111000111000000111110100 + 100000001001101011100101$

$a = 11111100011101000001110011011001$

$a = FC741CD9$

Maka putaran $t=0$ hash code dari pesan “735” yaitu:

Tabel 4.5. Nilai Putaran

	a	b	c	d	e	f	g	h
init	6a09e667	bb67ae85	3cbef372	a54ff53a	510e527f	9b05688c	1f83d9ab	5be0c019
t=0	ff0c8fcd	6a09e667	bb67ae85	3cbef372	a54ff53a	510e527f	9b05688c	1f83d9ab

7) *Compute intermediate hash value + initial hash value*

Setelah didapat ke 64 putaran dari hash computation, kemudian pada tahap ini dilakukan proses penjumlahan hasil putaran yang ke-64 dengan initial hash value. Maka hasil yang didapatkan adalah sebagai berikut:

$$H0(0) = 1b88f40d + 6a09e667 = 1a42d526$$

$$H0(1) = 3e8fhh40 + bb67ae85 = 7aba37d7$$

$$H0(2) = Fa88g0h1 + 3c6ef372 = 057cadd6$$

$$H0(3) = A1fgd244 + a54ff53a = 72fefef0$$

$$H0(4) = Dd1hg34e + 510e527f = 4771be24$$

$$H0(5) = F801eh5d + 9b05688c = 76eeee23$$

$$H0(6) = b0ffh23g + 1f83d9ab = 82710819$$

$$H0(7) = 10f2dda8 + 5be0cd19 = e1f57733$$

8) *Penggabungan H0 - H7*

$$H0 || H1 || H2 || H3 || H4 || H5 || H6 || H7$$

$$1a42d526 || 7aba37d7 || 057cadd6 || 72fefef0 || 4771be24 || 76eeee23 || 1d6f56a8 || e1f57733$$

9) *Nilai Hash*

Maka dengan seluruh proses yang dilalui didapatlah nilai hash sebagai berikut:
1a42d5267aba37d7057cadd672fefef04771be2476eeee231d6f56a8e1f57733

Hash code yang telah dienkripsi dengan SHA-256 ini selanjutnya akan dikombinasi dengan algoritma bcrypt untuk melindungi dari serangan Decode Hash.

4.5 Bcrypt

Bcrypt adalah hashing password dengan jumlah iterasi yang ditingkatkan untuk membuatnya lebih lambat dan bertahan lama terhadap serangan pencarian brute force juga meningkatkan daya komputasi dengan menggabungkan salt untuk melindungi terhadap serangan rainbow table.

Fungsi bcrypt adalah algoritma password hash default untuk OpenBSD dan sistem lainnya termasuk beberapa distribusi linux seperti SUSE Linux. Awalan dari

jenis Algoritma Bcrypt “\$2a\$” atau “\$2b\$” atau “\$2y\$” dalam string hash dalam file kata kunci bayangan menunjukkan bahwa string hash adalah hash Bcrypt dalam format kriptografi modular. Sisa dari string hash mencakup parameter biaya, salt 128 bit (basis-64 yang dikodekan sebagai 22 karakter), dan 192 bit dari nilai hash yang dihasilkan (basis-64 di kodekan sebagai 31 karakter).

4.5.1 Salt

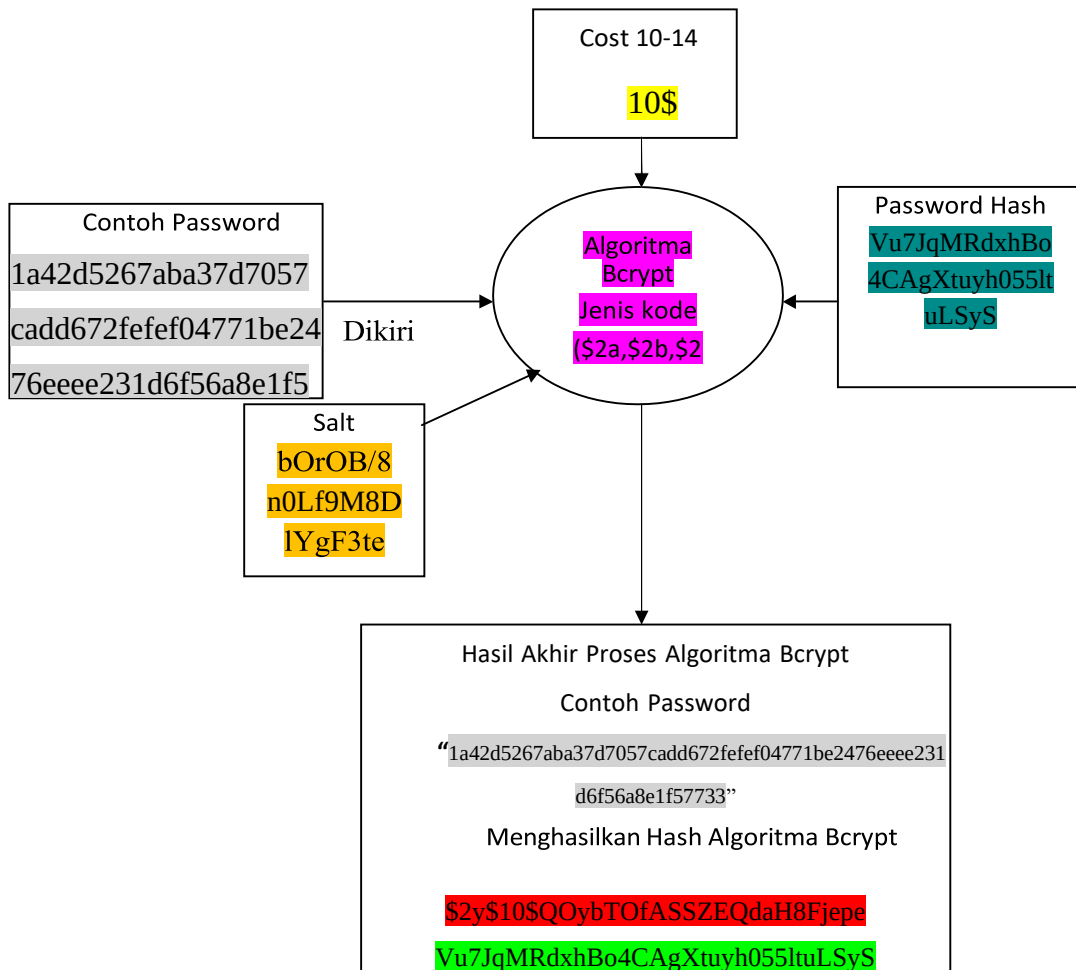
Salt adalah karakter acak yang akan di tambahkan di dalam proses enkripsi sebuah key. Salt berfungsi melapisi dan menjaga keamanan sebuah data yang telah di enkripsi, terutama dari dictionary-attack dan juga brute force.

4.5.2 Cost

Cost adalah jumlah hashing acak yang dijalankan dengan jumlah minimal cost 10 sampai 31 dan bahkan bisa lebih. (Buchanan, W.J., 2017)

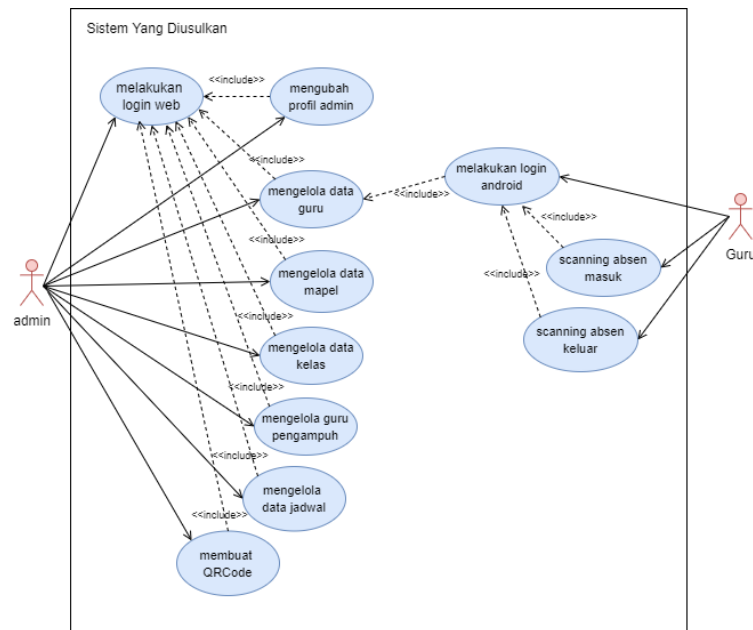
4.5.3 Proses Pengamanan Password Dengan Algoritma Bcrypt

Pada tahap ini penulis akan memberikan gambaran bagaimana password bcrypt yang telah dibuat diamankan oleh algoritma bcrypt berikut gambaran proses mengamankan password bcrypt. Password yang akan kita amankan adalah hasil hash pada SHA-256 yang telah kita proses di atas



4.6 Pembangunan Sistem

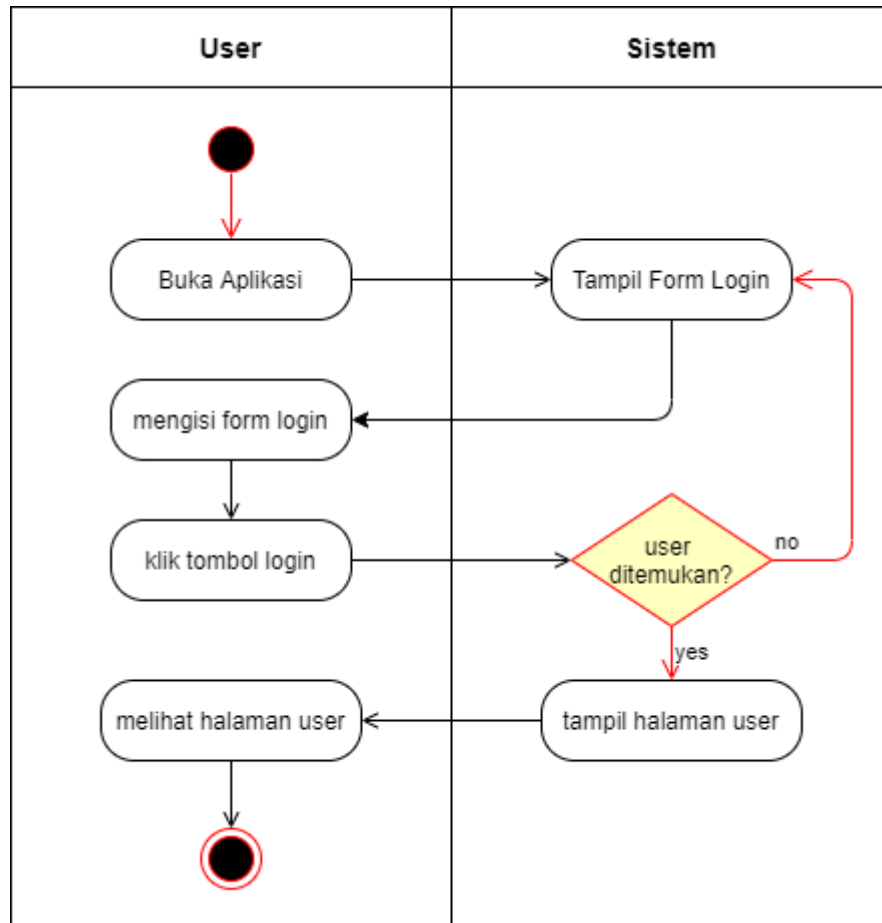
Aplikasi yang akan dibuat didesain menggunakan bahasa pemodelan *visual* dengan metode UML (*Unified Modelling Language*) sehingga dapat dijabarkan dalam bentuk yang baku dan mudah dimengerti:



Gambar 4.2. Sistem yang diusulkan

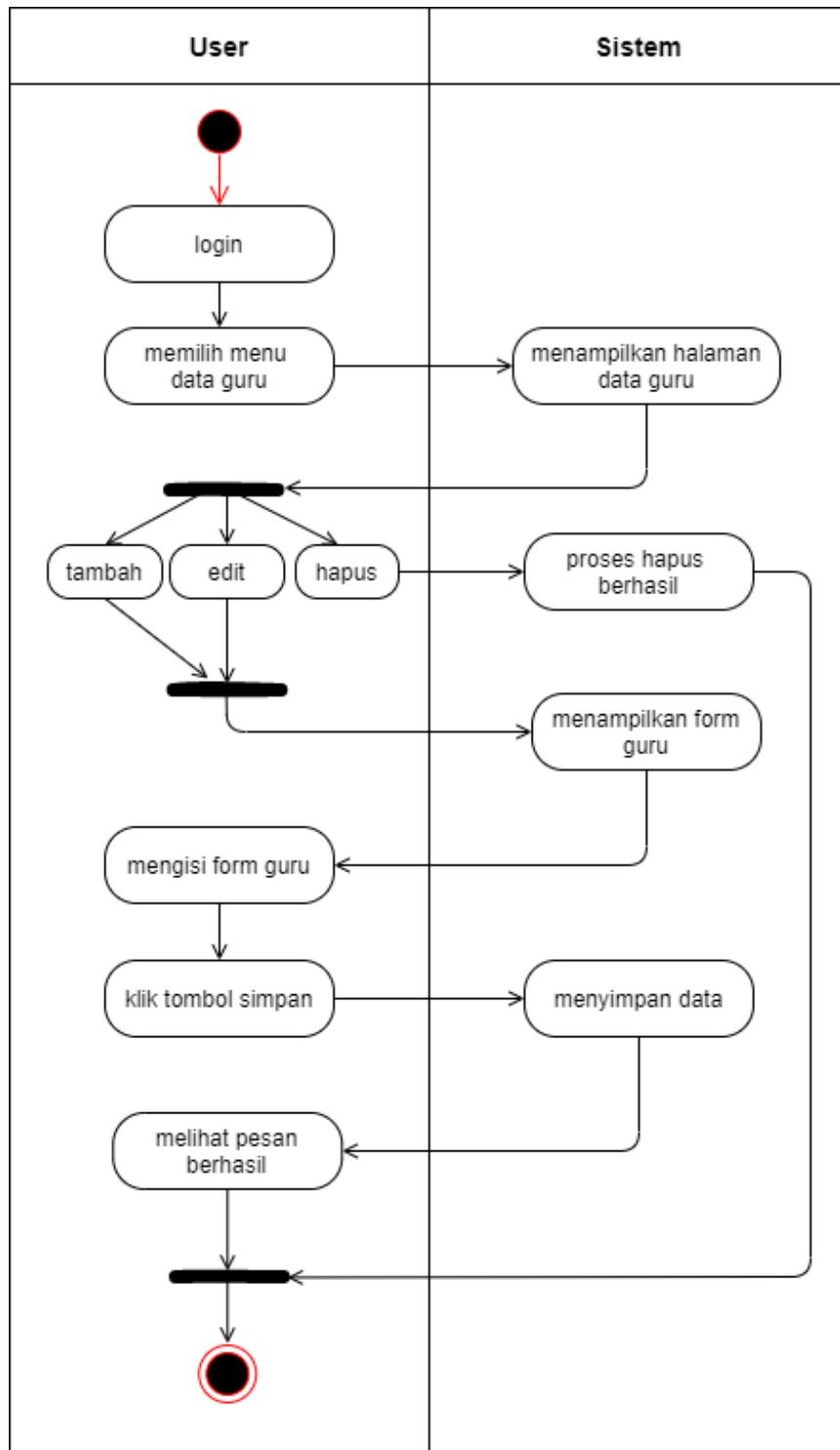
Berdasarkan gambar 4.2 dapat dideskripsikan bahwa sistem yang di usulkan terdapat 2 Aktor, yaitu admin, guru. *Behavior* admin pada *usecase* yaitu melakukan login web yang selanjutnya setelah login dapat mengubah profil admin, mengelola data guru, mengelola data mapel, mengelola data kelas, mengelola data guru pengampuh, mengelola data jadwal dan membuat *Quick Response Code*. Kemudian aktor Guru dapat melakukan scanning *Quick Response Code*. Aktor guru harus melakukan login android terlebih dahulu agar dapat melakukan scanning absen masuk dan absen keluar.

4.7 Activity Diagram Login



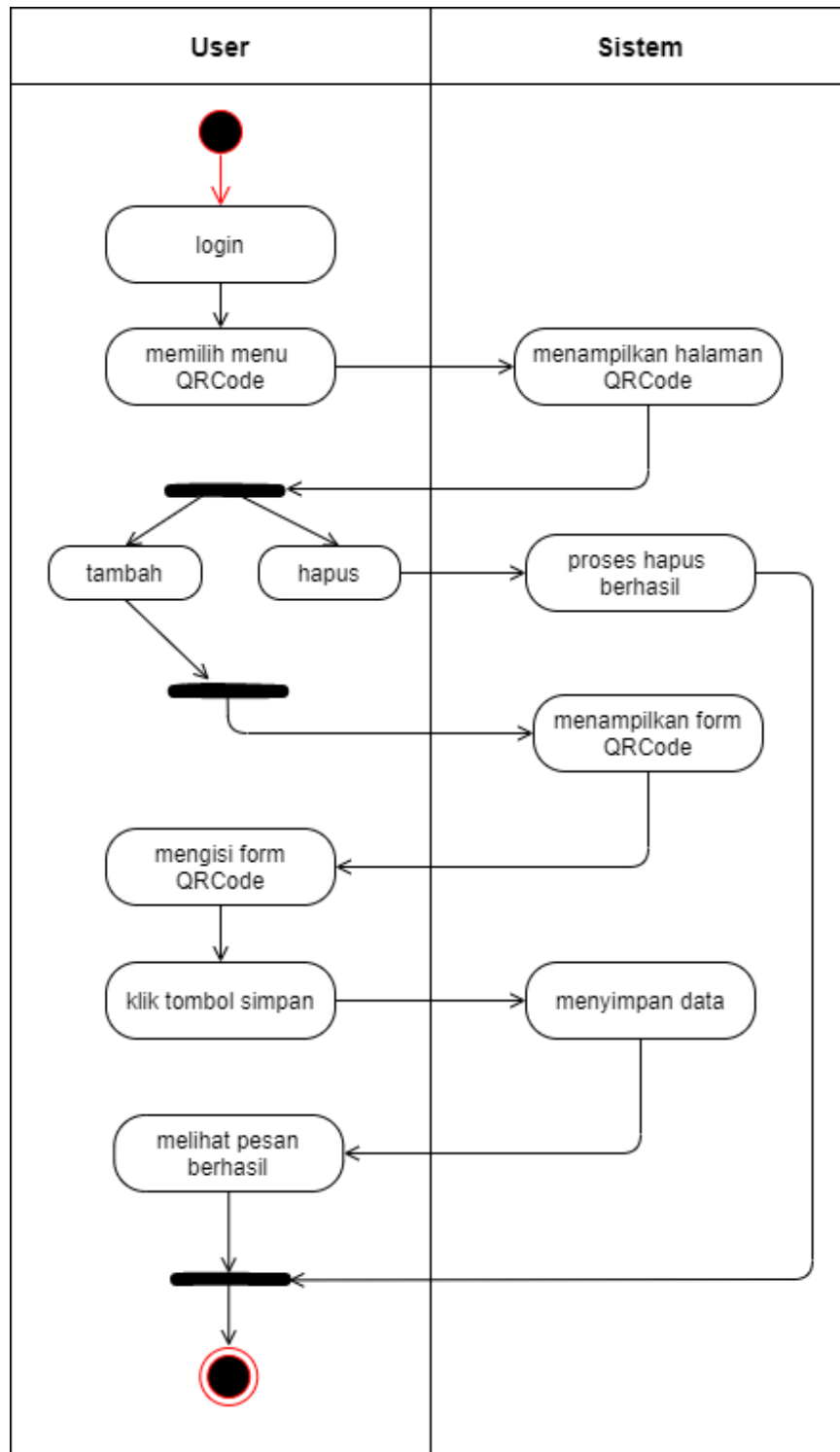
Gambar 4.3. Activity Diagram Login

4.8 Activity Diagram Kelola Data Guru



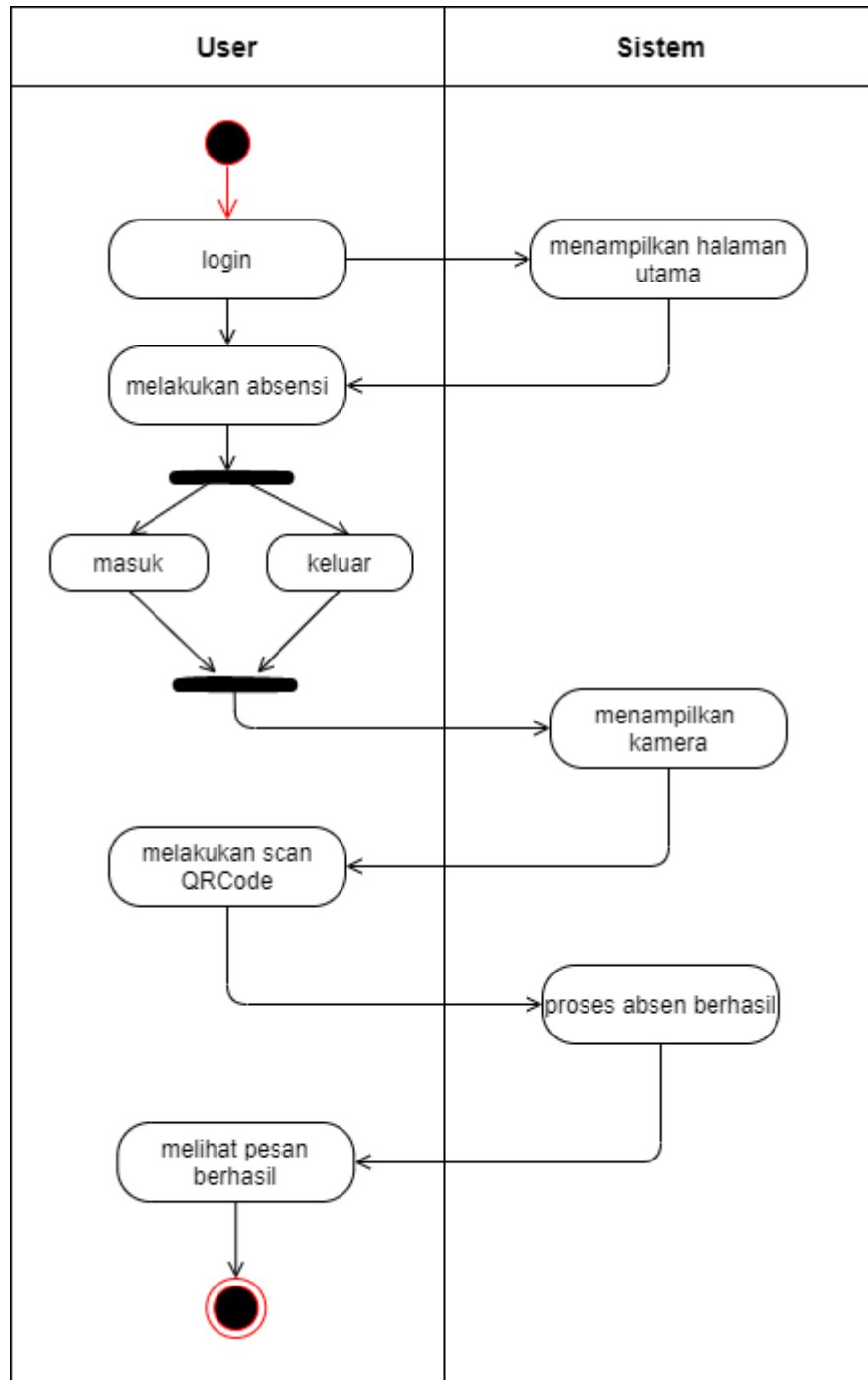
Gambar 4.4. Activity Diagram Kelola Data Guru

4.9 Activity Diagram Buat QRCode



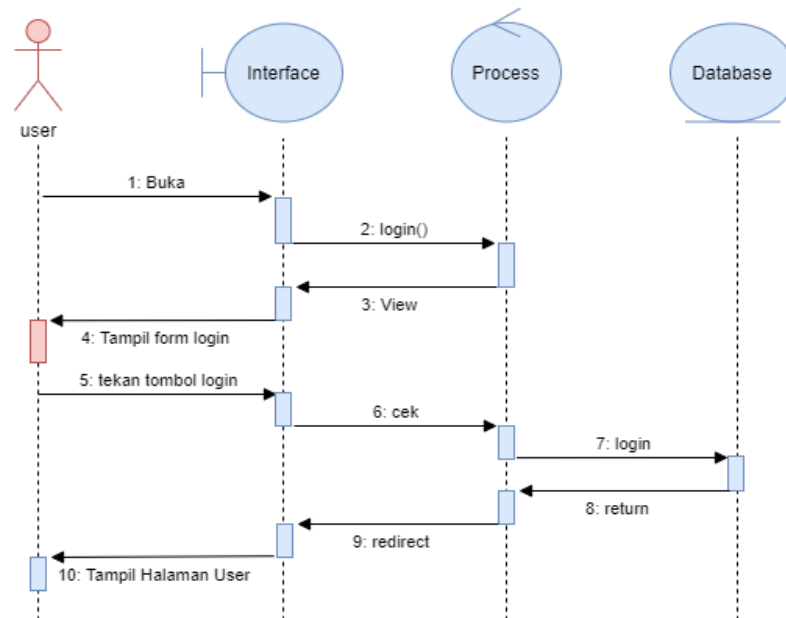
Gambar 4.5. Activity Diagram Buat *Quick Response Code*

4.10 Activity Diagram Scan Quick Response Code



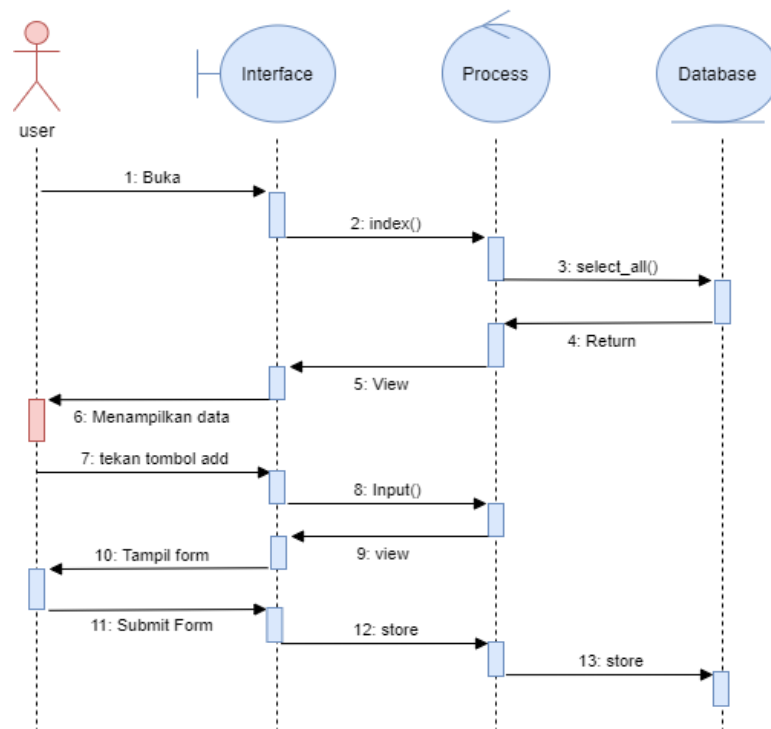
Gambar 4.6. Activity Diagram Scan Quick Response Code

4.11 Sequence Diagram Login



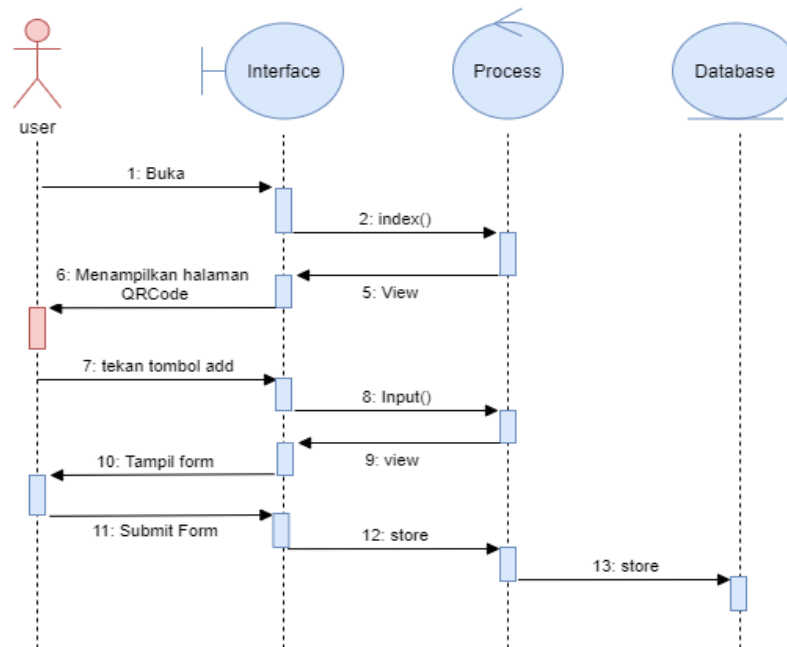
Gambar 4.7. Sequence Diagram Login

4.12 Sequence Diagram Kelola Data Guru



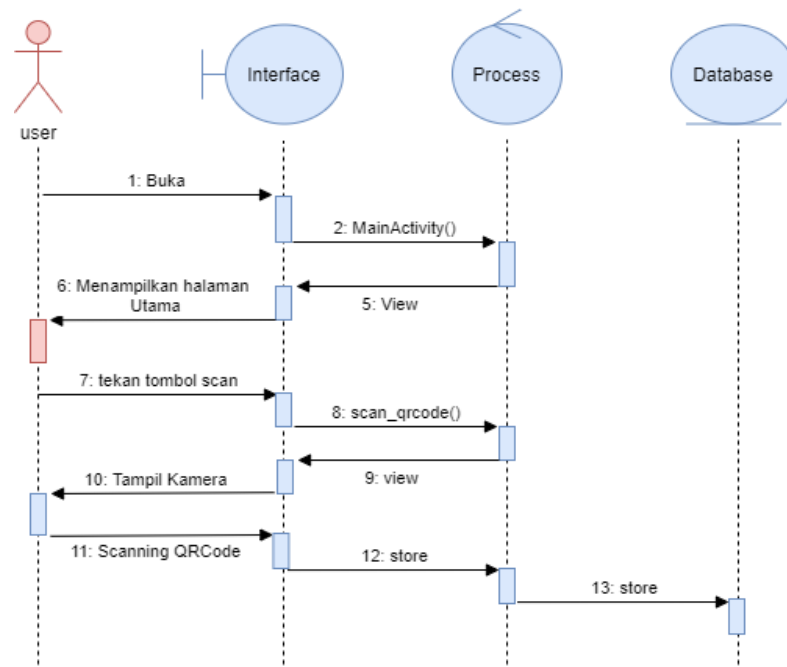
Gambar 4.8. Sequence Diagram Kelola Data Guru

4.13 Sequence Diagram Buat Quick Response Code



Gambar 4.9. Sequence Diagram Buat Quick Response Code

4.14 Sequence Diagram Scan Quick Response Code



Gambar 4.10. Sequence Diagram Scan Quick Response Code

4.15 Arsitektur Sistem

Untuk mendapatkan kinerja yang lebih optimal dalam pembuatan sistem disarankan menggunakan perangkat keras dan perangkat lunak sebagai berikut:

- 1) Processor : Intel Core i3 8300H
- 2) RAM : 4 GB
- 3) VGA : NVIDIA GeForce GTX 1050
- 4) SSD : 256 GB
- 5) Operating System : Windows 10
- 6) Tools : Android Studio, Sublime Text

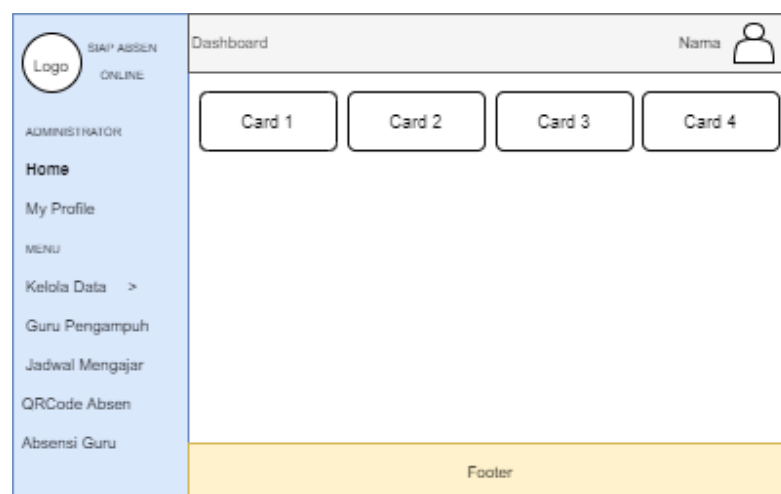
4.16 Interface Design

4.16.1 Mekanisme User

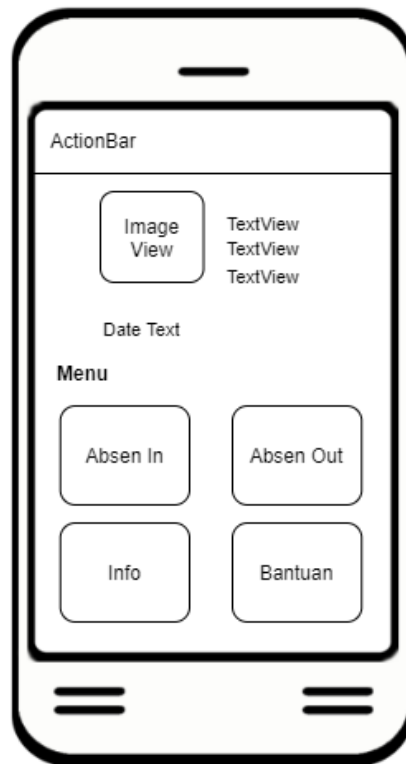
Tabel 4.6. Mekanisme User

User	Kategori	Akses Input	Akses Output
Guru	User	Scan QRCode	Menu Home
Admin	Administrator	All	All

4.16.2 Mekanisme Navigasi Home

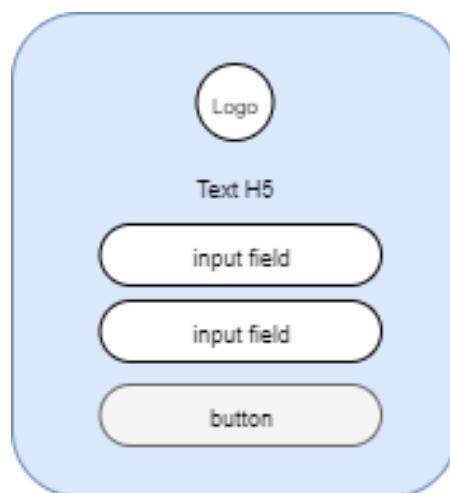


Gambar 4.11. Mekanisme Home Admin



Gambar 4.12. Mekanisme Navigasi Home Guru

4.16.3 Mekanisme Login



Gambar 4.13. Mekanisme Login Admin



Gambar 4.14. Mekanisme Login Guru

4.16.4 Mekanisme Input Data Guru

Form Guru

input field NIP

input field Nama

input field JenKel

input field TTL

input field Alamat

input field Foto

btn cancel

btn save

Gambar 4.15. Mekanisme Input Data Guru

4.16.5 Mekanisme Hapus dan Ubah Data Guru

Show

10

Entries

Search

#	NIP	Nama	Alamat	Jenkel	TTL	Foto	Action
1	value	value	value	value	value	value	
2	value	value	value	value	value	value	

Gambar 4.16. Mekanisme Hapus dan Ubah Data Guru

4.16.6 Mekanisme Buat *Quick Response Code*

Form Buat QRCode

input field kode

Label Warning

btn cancel

btn save

Gambar 4.17. Mekanisme Buat QRCode



4.16.7 Mekanisme Output

Gambar 4.18. Mekanisme Output

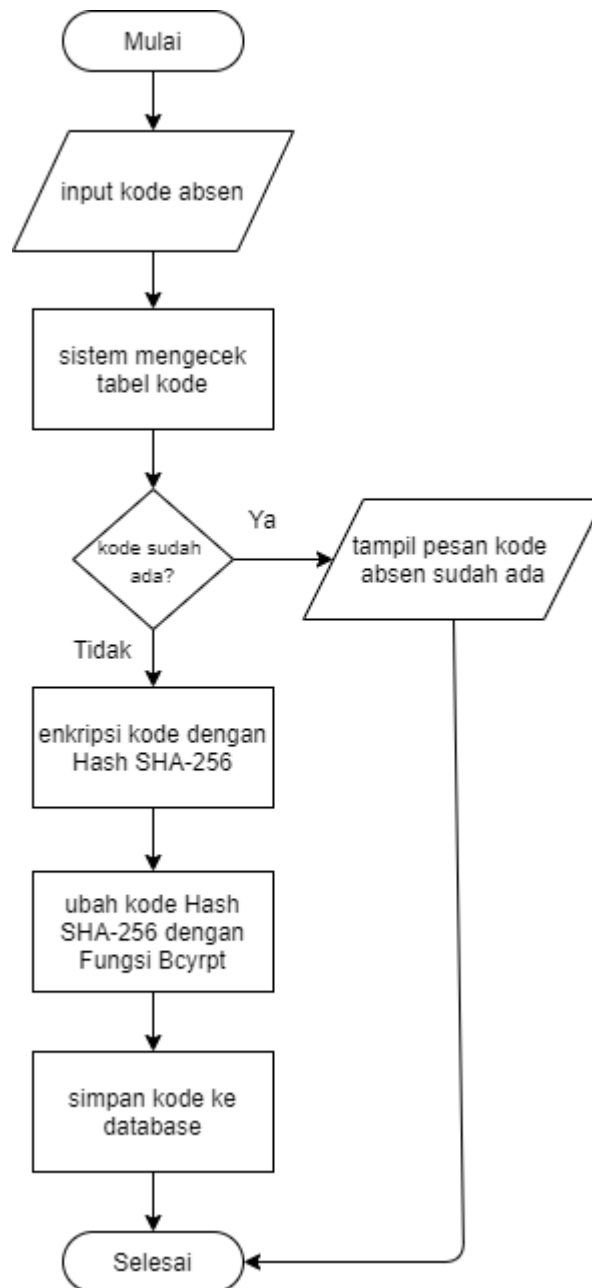
4.17 Hasil Pengujian Sistem

4.17.1 Pengujian White Box

Tabel 4.7. Pseudocode Proses Input *Quick Response Code*

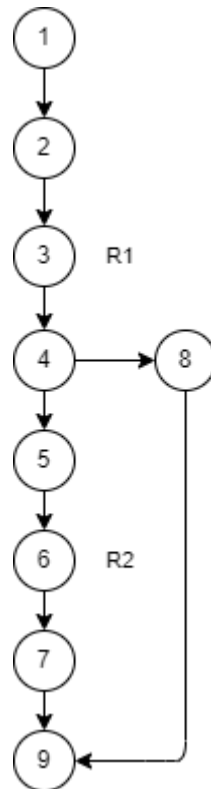
Node	Script
1	<code><?php echo form_open_multipart('qrkode/input');?></code>
2	<code><div class="modal-body"><div class="form-group"><div class="alert alert-warning" role="alert"> Anda yakin ingin membuat qrkode baru untuk dapat di scan saat absensi guru? klik tombol create dibawah jika anda benar-benar yakin.</div></div></div><div class="modal-footer"><button type="button" class="btn btn-danger" data-dismiss="modal"><i class="fas fa-fw fa-window-close"></i> &nbsp;Batal</button><button type="submit" class="btn btn-success"><i class="fas fa-fw fa-save"></i>&nbsp;Create</button></div></code>
3	<code>\$cek = \$this->db->get('tb_qrcode')->num_rows();</code>
4	<code>if (\$cek > 0) {</code>
8	<code>\$this->session->set_flashdata('message', '<div class="alert alert-danger" role="alert">&times;Hapus QRCode yang ada terlebih dahulu!</div>'); \$this->session->set_flashdata('kode_gagal', 'gagalModal'); \$this->session->set_flashdata('pesan_gagal', 'Maaf, Pembuatan QRCode untuk Absensi hanya dibatasi 1 saja!'); redirect('qrkode'); }</code>
5	<code>else { \$kode = \$this->input->post('kode'); \$enkrip_sha256 = hash("sha256", \$kode);</code>
6	<code>\$hash_bcrypt = password_hash(\$enkrip_sha256, PASSWORD_DEFAULT);</code>
7	<code>\$data = ['kode_absen' => htmlspecialchars(\$hash_bcrypt), 'created' => time()]; \$this->db->insert('tb_qrcode', \$data);</code>
9	<code>redirect('qrkode'); } }</code>

4.17.2 FlowChart



Gambar 4.19. Flowchart

4.17.3 Flowgraph Pengujian White Box



Gambar 4.20. Flowgraph

4.17.4 Perhitungan CC Pada Pengujian White Box

Dari Flowgraph tersebut didapatkan:

Diketahui: Region (R) = 2

Node (N) = 9

Edge (E) = 9

Predikat Node (P) = 1

Rumus: $V(G) = E - N + 2$ dan $V(G) = P + 1$

$V(G) = 9 - 9 + 2 = 2$

$V(G) = 1 + 1 = 2$

4.17.5 Perhitungan Basis Path Pada Pengujian White Box

Tabel 4.8. Basis Path

No	Path	Ket
1	1-2-3-4-5-6-7-9	OK
2	1-2-3-4-8-9	OK

Ketika Programnya dijalankan , maka akan terlihat bahwa semua basis path yang telah dihasilkan dieksekusi satu kali. Menurut ketentuan dari segi kelayakan program, system ini sudah memenuhi syarat.

4.17.6 Pengujian Black Box

Tabel 4.9. Tabel Pengujian *Blackbox* Admin

Input/Event	Fungsi	Hasil yang diharapkan	Hasil Uji
Buka Aplikasi	Masuk ke halaman utama	Tampil form login	Sesuai
Masukkan username salah dan klik login	Melakukan validasi user	Menampilkan pesan “username salah”	Sesuai
Masukkan Password salah dan klik login	Melakukan validasi password	Menampilkan pesa “password salah”	Sesuai
Masukkan username dan password benar, klik login	Melakukan validasi username dan password	Menampilkan halaman utama user	Sesuai
Klik menu Data Guru	Menampilkan data guru	Tampilkan data guru - edit / hapus	Sesuai
Ubah data guru	Mengubah data guru	Tampil pesan “Data berhasil diperbaharui”	Sesuai
Klik hapus pada kolom data guru	Menghapus data guru	Tampil pesan “Data berhasil dihapus”	Sesuai

Input/Event	Fungsi	Hasil yang diharapkan	Hasil Uji
Klik tambah data guru	Menambah data guru	Tampil form tambah data guru	Sesuai
Masukkan data guru, Klik simpan	Menyimpan data guru	Tampil pesan “Data berhasil disimpan”	Sesuai
Klik buat QRCode Absen	Menambah data QRCode	Tampil form tambah data QRCode	Sesuai
Masukkan Kode, Klik simpan	Menyimpan data QRCode	Tampil pesan “QRCode berhasil dibuat”	Sesuai

Tabel 4.10. Tabel Pengujian *Blackbox* Guru

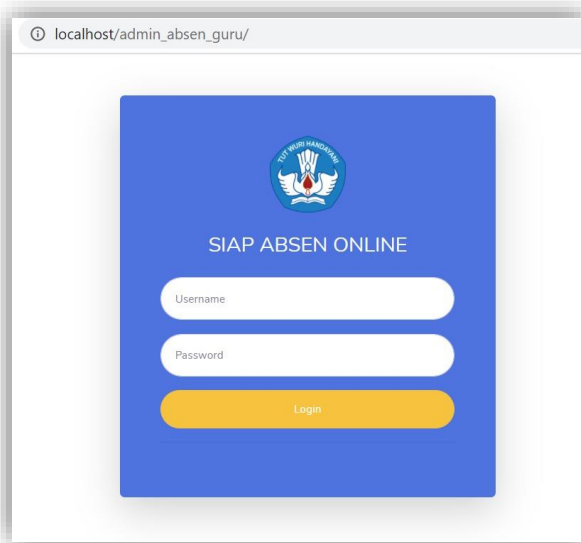
Input/Event	Fungsi	Hasil yang diharapkan	Hasil Uji
Buka Aplikasi	Masuk ke halaman utama	Tampil form login	Sesuai
Masukkan username salah dan klik login	Melakukan validasi user	Menampilkan pesan “username salah”	Sesuai
Masukkan Password salah dan klik login	Melakukan validasi password	Menampilkan pesa “password salah”	Sesuai
Masukkan username dan password benar, klik login	Melakukan validasi username dan password	Menampilkan halaman utama user	Sesuai
Klik Menu Absen Masuk/Keluar	Menampilkan Kamera Belakang	Menampilkan Kamera belakang untuk scanning	Sesuai
Scanning QRCode	Melakukan absensi QRCode	Tampil pesan “Anda berhasil absen masuk/keluar”	Sesuai
Klik Menu Bantuan	Menampilkan informasi bantuan	Tampil pesan “bantuan”	Sesuai

BAB V

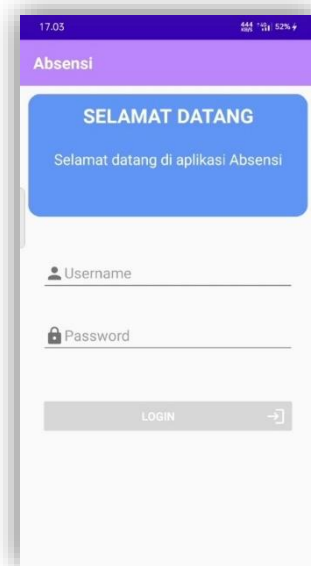
HASIL DAN PEMBAHASAN

5.1 Pembahasan Sistem

5.1.1 Tampilan Login



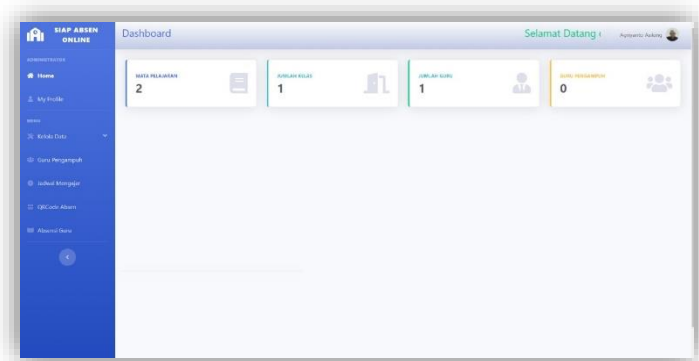
Gambar 5.1. Tampilan Login Admin



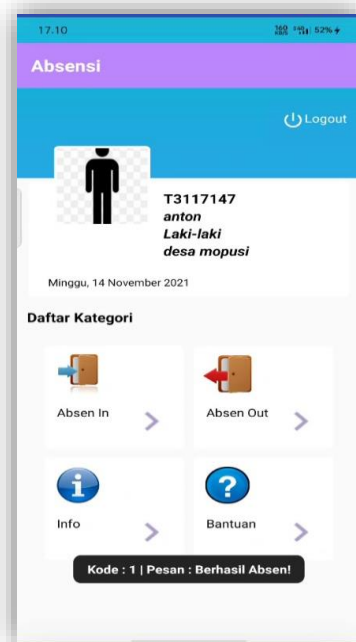
Gambar 5.2. Tampilan Login Guru

Halaman pada gambar 5.1 digunakan untuk login admin dengan memasukkan username dan password kemudian menekan tombol login, sedangkan gambar 5.2 digunakan oleh guru untuk login guru dengan memasukkan username dan password dan menekan tombol login.

5.1.2 Tampilan Halaman Utama



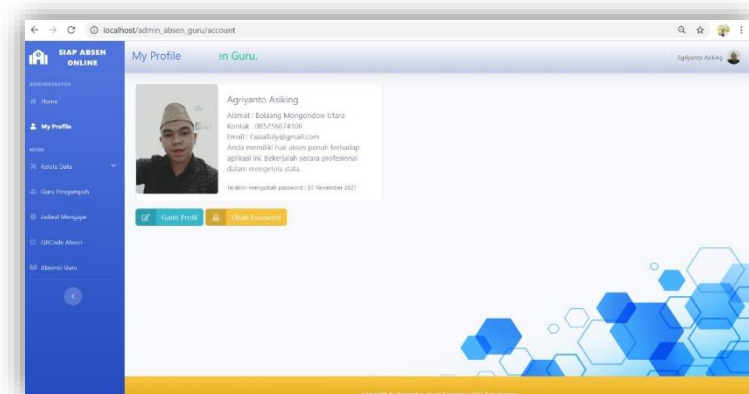
Gambar 5.3. Tampilan Halaman Utama Admin



Gambar 5.4. Tampilan Halaman Utama Guru

Gambar 5.3 adalah halaman utama saat admin berhasil login, sedangkan gambar 5.4 adalah halaman utama saat guru berhasil melakukan login.

5.1.3 Tampilan Profil Admin



Gambar 5.5. Tampilan Profil Admin

Gambar diatas merupakan halaman profil admin dan dapat diubah oleh admin itu sendiri.

5.1.4 Tampilan Tambah Data Guru

Gambar 5.6. Tampilan Tambah Data Guru

Halaman diatas digunakan untuk menambah data guru oleh admin.

5.1.5 Tampilan Buat Quick Response Code

Buat QRCode Absensi

Masukkan Kode

Anda yakin ingin membuat qrcode baru untuk dapat di scan saat absensi guru? klik tombol create dibawah jika anda benar-benar yakin.

Batal Create

Gambar 5.7. Tampilan Buat Quick Response Code
Halaman diatas digunakan untuk membuat *Quick Response Code* absensi oleh admin.

5.1.6 Tampilan Daftar Guru

SIAP ABSEN ONLINE

Kelola Data Sistem Informasi Pengelolaan Data Absen Guru.

Agrianto Asling

+ Tambah Data

Show 10 entries

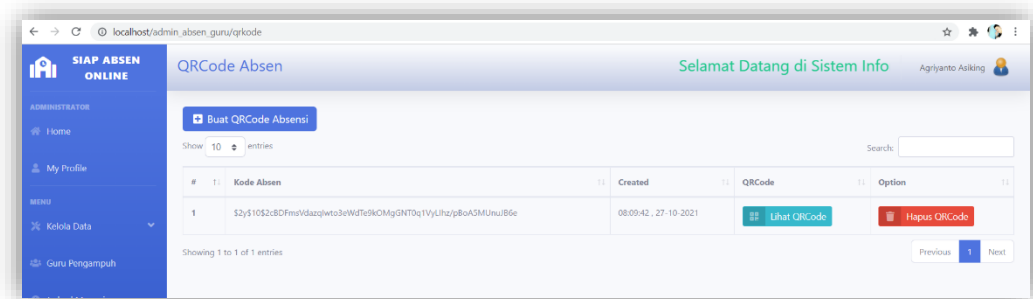
#	NIP	Nama	Alamat	Jenkel	Tempat Tanggal Lahir	Foto	Action
1	110200937001	Nur Anisa Aritula	Kota Gorontalo	Perempuan	Gorontalo, 29-06-1999		
2	110200000000	Aldal Yado, S.Kom	Limboto	Laki-laki	Manado, 29-06-1998		

Showing 1 to 2 of 2 entries

Previous 1 Next

Gambar 5.8. Tampilan Daftar Guru
Halaman ini menampilkan data guru yang telah diinput oleh admin dan dapat diedit atau dihapus.

5.1.7 Tampilan Data Quick Response Code



Gambar 5.9. Tampilan Data Quick Response Code

Halaman ini menampilkan *Quick Response Code* yang sudah dibuat oleh admin. *Quick Response Code* dapat dilihat dengan menekan tombol lihat qrcode pada kolom. QRCode juga bisa dihapus.

5.1.8 Proses Enkrip SHA-256

Pada proses ini penulis akan melakukan pembahasan pada proses Enkrip SHA-256 kemudian di amankan lagi dengan Bckrypt.

- 1) Langkah pertama yaitu input plain teks

Plain teks adalah sebuah kata atau karakter yang akan kita enkrip dengan SHA256 dan Bcrypt, Plain teks yang akan di buat oleh penulis yaitu : tes

- 2) Pada tahap ini pesan yang dimasukan oleh penulis tadi akan di ubah ke dalam bentuk angka biner agar bisa ke tahap selanjutnya.

t = 01110100

e = 01100101

s = 01110011

Setelah di ubah ke angka biner maka pesan “tes” tadi menjadi

M=011101000110010101110011

Diketahui panjang pesan = 24 bit

- 3) *Message Padding*

Padding pesan yang telah di ubah ke angka biner tadi dengan cara menambahkan bit 1 dan sisanya bit nol hingga pesan sepanjang 512 bit. Untuk menemukan berapa bit nol yang akan ditambahkan maka laukan dengan rumus :

$$I + 1 + k = 448 \text{ mod } 512$$

$$k = 448 - 25 \text{ mod } 512$$

$$24 + 1 + k = 448 \text{ mod } 512$$

$$k = 423$$

Karena $K = 423$ maka banyaknya bit 0 yang akan ditambahkan adalah sebanyak 423 bit.

4) *Parsing*

Pesan yang telah dipadding menghasilkan blok pesan 512 bit selanjutnya adalah melakukan pembagian setiap blok 512 bit menjadi 16 buah word 32 bit.

5) *Message Schedule*

Tahap ini adalah memperluas memperluas masing-masing 16 buah word yang telah diparsing menjadi 64 buah 32 bit word.

6) *Inisialisasi Variabel dan Konstanta*

Tahap kita hanya perlu menuliskan variabel awal pada fungsi SHA-256 kemudian kita inisialisasikan, yaitu sebagai berikut:

$$a = H_0(0) = 6A09E667$$

$$b = H_0(1) = BB67AE85$$

$$c = H_0(2) = 3C6EF372$$

$$d = H_0(3) = A54FF53A$$

$$e = H_0(4) = 510E527F$$

$$f = H_0(5) = 9B05688C$$

$$g = H_0(6) = 1F83D9AB$$

7) *Hash Computation*

Dalam proses ini dilakukan perhitungan nilai a sampai h sebanyak 64 kali putaran.

8) *Compute intermediate Hash Value + Initial Hash Value*

Setelah didapat hasil ke 64 dalam proses *Hash Computation* kemudian dilakukan proses penjumlahan hasil ke-64 dengan nilai hash value.

9) *Penggabungan H0 – H7*

Tahap ini kita hanya perlu melakukan penggabungan hasil dari penjumlahan ke-64 dan hash value.

10) Nilai Hash

Dengan seluruh proses yang telah dilalui didapatkan nilai hash SHA-256 dari pesan tes:

ce0f6c28b5869ff166714da5fe08554c70c731a335ff9702e38b00f81ad348c6

5.1.9 Proses Bcrypt

Pada proses ini penulis akan melakukan pengaman hasil dari hash SHA-256 di atas dengan BCRYPT untuk menghindari serangan decode SHA-256.

1) plain teks password

Pada tahap ini penulis memasukan plain teks password yang telah di hash menggunakan SHA-256 yaitu :

ce0f6c28b5869ff166714da5fe08554c70c731a335ff9702e38b00f81ad348c6

2) Cost

Memasukan jumlah hashing acak yang dijalankan dengan jumlah minimal cost 10 sampai 30

3) Salt

Menambahkan karakter acak yang akan di tambahkan di dalam proses enkripsi sebuah key. Salt berfungsi melapisi dan menjaga keamanan sebuah data yang telah di enkripsi.

4) Proses *Hashing*

melakukan proses plaintext yang telah di inputkan agar terbentuk ke dalam algoritma hash yaitu algoritma Bcrypt yang di gunakan oleh penulis dengan besaran 192 bit proses hash yang dihasilkan.

5) Hasil bcrypt, cost, salt dan hash

Hasil dari proses bcrypt, cost, salt dan hash yaitu:

Bcrypt = \$2y\$

Cost = 10\$

Salt = aSjYS2ng96ouyDPDEkA1R

Hash =eQar2UoRWOlwJwVuc2.Fe7/pbcGbOFva

6) Hasil akhir

Hasil dari pesan hash SHA-256 yang di amankan dengan BCRYPT yaitu:

\$2y\$10\$aSjYS2ng96ouyDPDEkA1ReQar2UoRWOlwJwVuc2.Fe7/pbcGb
OFva

5.1.10 Tampilan Hasil Proses SHA-256 Dan BCRYPT

Show 10 entries

#	Kode Absen
1	\$2y\$10\$aSjYS2ng96ouyDPDEkA1ReQar2UoRWOlwJwVuc2.Fe7/pbcGbOFva

Gambar 6.0. Tampilan Hasil Proses SHA-256 dan BCRYPT

BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan penelitian yang dilakukan implementasi SHA-256 pada *Quick Response Code* absensi dan pembahasan yang sudah diuraikan sebelumnya, kesimpulan yang diperoleh:

1. Sistem yang dirancang mampu melakukan *generate Quick Response Code* dan *Scan Quick Response Code* untuk absensi melalui *smartphone android* sehingga meminimalisir kontak fisik atau penggunaan benda yang disentuh oleh orang banyak sehingga mengurangi potensi penyebaran virus COVID-19.
2. Pengamanan *Quick Response Code* dengan menggunakan enkripsi SHA-256 lebih optimal dengan mengkombinasikan fungsi BCrypt pada Message yang telah dienkripsi SHA-256, sehingga menghindari serangan decode hash SHA-256.

6.2 Saran

Setelah melakukan penelitian dan pembuatan suatu program untuk mengoptimalkan keamanan *Quick Response Code* absensi dengan menggunakan SHA-256 dan dikombinasi dengan Fungsi Hash BCrypt untuk, maka:

1. Diharapkan pengembangan aplikasi untuk menambahkan fitur Geolocation untuk mengukur radius user agar absensi hanya dapat dilakukan di wilayah sekolah.
2. Penelitian kedepannya diharapkan menggunakan algoritma kriptografi yang berbeda dan kombinasi yang berbeda juga untuk menghasilkan penelitian yang lebih baik lagi.

DAFTAR PUSTAKA

- [1] Q. Aini, Y. I. Graha and S. R. Zuliana, "Penerapan Absensi QRCode Mahasiswa Bimbingan Belajar pada Website berbasis Yii Framework," Jurnal Ilmiah Sistem Informasi dan Teknik Informatika, vol. VII, 2017.
- [2] Q. Aini, U. Rahardja and A. Fatillah, "Penerapan QR Code Sebagai Media Pelayanan Untuk Absensi Pada Website Berbasis PHP Native," Jurnal Ilmiah Sistem Informasi dan Teknik Informatika, vol. VIII, 2018.
- [3] A. Nashir, "Pengaruh Kedisiplinan Guru Terhadap Prestasi Belajar," Jurnal Tarbawi, vol. I, 2016.
- [4] Y. Supendi, I. Supriadi and A. A. Isto, "Pemanfaatan Teknologi QR Code Pada Sistem Presensi Mahasiswa Berbasis Mobile," Seminar Nasional Aptikom, 2019.
- [5] Y. A. Sujarwo and A. Ratnasari, "Aplikasi Reservasi Parkir Inap Menggunakan Metode Fishbone Diagram dan QR Code," Jurnal Sistem Informasi dan Komputer, vol. IX, pp. 302-309, 2020.
- [6] R. Damanik, "Pengkodean Pesan Teks Dengan Proses Penerapan Algoritma Kriptografi Secure Hash Algorithm (SHA)," Jurnal Informatika Kaputama, vol. I, 2017.
- [7] E. K. Suni and H. I. Maulana, "Penerapan Digital Signature Untuk Mengesahkan Proposal Hibah Dikti Menggunakan Secure Hash Algorithm," Journal of Information Technology and Computer Science, vol. V, pp. 105-112, 2020.

- [8] A. Pariddudin and F. Syauqi, "Penerapan Algoritma AES pada QR Code Untuk Keamanan Verifikasi Tiket," *Jurnal Ilmiah Teknologi - Informasi dan Sains*, vol. X, pp. 43-52, 2020.
- [9] I. Wijaya, D. E. Herwindiati and J. Hendryli, "Smart Presensi Menggunakan QR Code dengan Secure Hash Algorithm 2 (SHA-2)," *Jurnal Ilmu Komputer dan Sistem Informasi*, vol. IX, 2021.
- [10] M. Khoiriyah, H. L. Purwanto and Y. S. Dwanoko, "Rancang Bangun Presensi Perkuliahan Menggunakan QRCode (Studi Kasus Fakultas Sains dan Teknologi Universitas Kanjuruhan Malang)," *Jurnal Terapan Sains dan Teknologi*, vol. I, 2019.
- [11] F. Saeful Gani, "Implementasi Quick Respon Code Pada Aplikasi Inventarisasi Barang Berbasis Android," Thesis Universitas Siliwangi, 2020.
- [12] M. D. Setiadi and N. Rosmawarni, "Perancangan Aplikasi QR Code Sebagai Media Informasi Pengenalan Satwa Kebun Binatang Berbasis Website," *Jurnal Rekayasa*, vol. IX, 2020.
- [13] R. Habibi, D. Anik Masruro and N. H. Khonsa, *Aplikasi Inventory Barang Menggunakan QR Code*, Bandung: Informatics Research Center, 2020.
- [14] Yuntriani and A. K. Hasyim, "Sistem Informasi Absensi Harian Smpn 01 Abung Tinggi Menggunakan Metode Waterfall Untuk Meningkatkan Kedisiplinan Siswa," *Jurnal Manajemen Pendidikan Al Multazam*, vol. I, 2019.
- [15] A. hamid, "Guru Profesional," *Jurnal Al Falah*, vol. XVII, 2017.
- [16] R. K. Ibrahim, "Incorporating Sha-2 256 With OFB To Relize A Novel Encryption Method," *World Symposium on Computer Network and Information Security (WSCNIS) Hammamet*, pp. 19-21, 2015.

- [17] C. P. Sukhbir, "Crypto Currencies for Digital Currency Using Cipher Text and SHA256," *Journal of Adv Research in Dynamical & Control Systems*, pp. 530-534, 2017.
- [18] Z. Panjaian, E. F. Ginting and Yusnidah, "Modifikasi SHA-256 dengan Algoritma Hill Cipher untuk Pengamanan Fungsi Hash dari Upaya Decode Hash," *Jurnal Sains Manajemen Informatika dan Komputer*, vol. XIX, pp. 53-61, 2020.
- [19] Herlinah and Musliadi, *Pemrograman Aplikasi Android Dengan Android Studio, Photoshop, dan Audition*, Jakarta: PT. Elex Media Komputindo, 2019.
- [20] R. Rizal and A. Rahmatulloh, "RESTful Web Service untuk Integrasi Sistem Akademik dan Perpustakaan Universitas Perjuangan," *Jurnal Ilmiah Informatika*, vol. VII, 2019.
- [21] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," *Jurnal Format*, vol. VI, 2016.
- [22] J. Karman, H. Mulyono and T. Martadinata, *Sistem Informasi Geografis Berbasis Android Studi Kasus Aplikasi SIG Pariwisata*, Yogyakarta: Deepublish, 2019.
- [23] J. Enterprise, *Pengenalan HTML dan CSS*, Jakarta: PT Elex Media Komputindo, 2016.
- [24] M. MF, *Buku Sakti Pemrograman Web Seri PHP*, Yogyakarta: Startup, 2018.
- [25] M. S. Novendri, "Aplikasi Inventaris Barang Pada Mts Nurul Islam Dumai Menggunakan Php Dan Mysql," *Jurnal Lentera Dumai*, vol. X, 2019.

- [26] I. T. Kusnadi, A. Supiandi, R. N. Syabaniah and R. Oktapiani, *Pemodelan Sistem Berbasis Objek With UML*, Yogyakarta: Graha Ilmu, 2019.
- [27] W. N. Cholifah, Yulianingsih and S. M. Sagita, "Pengujian Black Box Testing Pada Aplikasi Action & Strategy Berbasis Android Dengan Teknologi Phonegap," *Jurnal String*, vol. III, pp. 206-210, 2018.
- [28] C. T. Pratala, E. M. Asyer, I. Prayudi and A. Saifudin, "Pengujian White Box pada Aplikasi Cash Flow Berbasis Android Menggunakan Teknik Basis Path," *Jurnal Informatika Universitas Pamulang*, vol. V, pp. 111-119, 2020.
- [29] R. Subagia, R. Alit and F. A. Akbar, "Pengujian Whitebox Pada Sistem Informasi Monitoring Skripsi Program Studi Informatika," *Jurnal Informatika dan Sistem Informasi*, vol. I, 2020.
- [30] T. Hidayat and M. Muttaqin, "Pengujian Sistem Informasi Pendaftaran dan Pembayaran Wisuda Online menggunakan Black Box Testing Dengan Metode Equivalence Partitioning dan Boundary Value Analysis," *Jurnal Teknik Informatika UNIS*, vol. VI, 2018.
- [31] B. Saputro, *Manajemen Penelitian Pengembangan (Research & Development) Bagi Penyusun Tesis Dan Disertasi*, Yogyakarta: Aswaja Pressindo, 2017.

LAMPIRAN

1. Absen.php

```
<?php
defined('BASEPATH') OR exit('No direct script access allowed');
class Absen extends CI_Controller
{
    public function __construct()
    {
        parent::__construct();
        if (!$this->session->userdata('username')) {
            redirect('auth');
        }
    }
    public function index()
    {
        $data['title'] = 'Absensi Guru';
        $data['user'] = $this->db->get_where('tb_admin', ['role' => $this->session->userdata('role')])->row_array();
        $this->db->join('tb_guru', 'tb_guru.id_guru=tb_absen.id_guru');
        $data['absen'] = $this->db->get('tb_absen')->result_array();
        $this->load->view('templates/header', $data);
        $this->load->view('templates/sidebar', $data);
        $this->load->view('templates/topbar', $data);
        $this->load->view('absen/index', $data);
        $this->load->view('templates/footer');
    }
}
```

2. Account.php

```
<?php
defined('BASEPATH') OR exit('No direct script access allowed');
class Account extends CI_Controller
{
    public function __construct()
    {
        parent::__construct();
        if (!$this->session->userdata('username')) {
            redirect('auth');
        }
    }
    public function index()
    {
```



```

        $data['title'] = 'My Profile';
        $data['user'] = $this->db->get_where('tb_admin', ['username' =>
$this->session->userdata('username')])->row_array();
        $this->load->view('templates/header', $data);
        $this->load->view('templates/sidebar', $data);
        $this->load->view('templates/topbar', $data);
        $this->load->view('account/index', $data);
        $this->load->view('templates/footer');
    }
    public function edit($id){
        $data['title'] = 'My Profile';
        $data['user'] = $this->db->get_where('tb_admin', ['role' => $this-
>session->userdata('role')])->row_array();
        $data['admin_data'] = $this->db->get_where('tb_admin', ['id' =>
$id])->row_array();
        $this->load->view('templates/header', $data);
        $this->load->view('templates/sidebar', $data);
        $this->load->view('templates/topbar', $data);
        $this->load->view('account/edit', $data);
        $this->load->view('templates/footer');
    }
    public function edit_proses(){
        $upload_image = $_FILES['gambar']['name'];
        if ($upload_image){
            $config['upload_path']      = './assets/img/profile/';
            $config['allowed_types']    = 'gif|jpg|png';
            $config['max_size']         = '4050';
            $this->load->library('upload', $config);
            if ($this->upload->do_upload('gambar')){
                $old_image = $this->input->post('gambar_lama');
                $new_image = $this->upload->data('file_name');
                unlink(FCPATH . 'assets/img/profile/' .
$old_image);
                $this->db->set('foto_admin', $new_image);
            }else {
                $this->session->set_flashdata('message', '<div
class="alert alert-danger" role="alert"><a href="" class="close" data-
dismiss="alert" aria-label="close">&times;</a>' . $this->upload-
>display_errors() . '</div>');

```

```

        $this->session->set_flashdata('kode_gagal',
'gagalModal');
        $this->session->set_flashdata('pesan_gagal', 'Gagal
unggah Foto, Pastikan jenis file PNG/JPG/JPEG!');
        redirect('account');
    }
}
$nama = $this->input->post('nama');
$alamat = $this->input->post('alamat');
$no_hp = $this->input->post('no_hp');
$email = $this->input->post('email');
$id = $this->input->post('id');
$this->db->set('nama', $nama);
$this->db->set('alamat', $alamat);
$this->db->set('email', $email);
$this->db->set('no_hp', $no_hp);
$this->db->set('date_created', time());
$this->db->where('id', $id);
$this->db->update('tb_admin');
$this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Update succeeded!</div>');
$this->session->set_flashdata('kode_berhasil', 'suksesModal');
$this->session->set_flashdata('pesan_berhasil', 'Data profil telah
diperbaharui!');
    redirect('account');
}
}

```

3. Auth.php

```

<?php
defined('BASEPATH') OR exit('No direct script access allowed');
class Auth extends CI_Controller
{
    public function __construct()
    {
        parent::__construct();
        $this->load->library('form_validation');
    }
    public function index()
    {

```

```

        $this->form_validation->set_rules('username', 'Username',
        'required|trim');
        $this->form_validation->set_rules('password', 'Password',
        'required|trim');
        if ($this->form_validation->run() == false){
            $data['title'] = 'Login Page';
            $this->load->view('templates/auth_header', $data);
            $this->load->view('auth/login');
            $this->load->view('templates/auth_footer');
        } else {
            // validasi sukses
            $this->_login();
        }
    }
    private function _login()
    {
        $username = $this->input->post('username');
        $password = $this->input->post('password');
        $user = $this->db->get_where('tb_admin', ['username' =>
        $username])->row_array();
        // cek usernya ada
        if ($user) {
            // cek password
            if (password_verify($password, $user['password']))
            {
                $data = [
                    'username' => $user['username'],
                    'role' => $user['role'] ];

                $this->session->set_userdata($data);
                redirect('user');
            } else {
                $this->session->set_flashdata('message', '<div
                class="alert alert-danger" role="alert"> Wrong password!</div>');
                redirect('auth');}
        } else {
            $this->session->set_flashdata('message', '<div class="alert
            alert-danger" role="alert"> Username tidak tersedia!</div>');
            redirect('auth');
        }
    }

```

```

    }
}
public function registration()
{

    $this->form_validation->set_rules('name', 'Name', 'required|trim');
    $this->form_validation->set_rules('email', 'Email',
'required|trim|valid_email|is_unique[user.email]', [
        'is_unique' => 'This email has already registered!'
    ]);
    $this->form_validation->set_rules('password1', 'Password',
'required|trim|min_length[5]|matches[password2]', ['matches' => 'Password
dont match!', 'min_length' => 'Password too short!']);
    $this->form_validation->set_rules('password2', 'Password',
'required|trim|matches[password1]');
    if ($this->form_validation->run() == false) {
        $data['title'] = 'WPU User Registration';
        $this->load->view('templates/auth_header', $data);
        $this->load->view('auth/registration');
        $this->load->view('templates/auth_footer');
    } else {
        $data = [
            'name' => htmlspecialchars($this->input-
>post('name', true)),
            'email' => htmlspecialchars($this->input-
>post('email', true)),
            'image' => 'default.jpg',
            'password' => password_hash($this->input-
>post('password1'), PASSWORD_DEFAULT),
            'role_id' => 2,
            'is_active' => 1,
            'date_created' => time()
        ];
        $this->db->insert('user', $data);
        $this->session->set_flashdata('message', '<div class="alert
alert-success" role="alert"> Congratulation! Your account has been created.
Please Login</div>');
        redirect('auth');
    }
}
}

```

```

public function logout()
{
    $this->session->unset_userdata('username');
    $this->session->unset_userdata('role');
    $this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"> You have been logout!</div>');
    redirect('auth');
}
}

```

4. Guru.php

```

<?php
defined('BASEPATH') OR exit('No direct script access allowed');

class Guru extends CI_Controller
{

    public function __construct()
    {
        parent::__construct();
        if (!$this->session->userdata('username')) {
            redirect('auth');
        }
    }

    public function index()
    {
        $data['title'] = 'Kelola Data';
        $data['user'] = $this->db->get_where('tb_admin', ['username' => $this-
>session->userdata('username')])->row_array();

        $this->db->order_by('id_guru', 'DESC');
        $data['guru'] = $this->db->get('tb_guru')->result_array();

        $this->load->view('templates/header', $data);
        $this->load->view('templates/sidebar', $data);
        $this->load->view('templates/topbar', $data);
        $this->load->view('guru/index', $data);
        $this->load->view('templates/footer');
    }
}

```

```

    }

    public function hapus($id){

        $data = $this->db->get_where('tb_guru', ['id_guru' => $id ])-
        >row_array();

        unlink(FCPATH . 'assets/img/gambar/' . $data['foto']);

        $this->db->where('id_guru', $id);
        $this->db->delete('tb_guru');
        $this->session->set_flashdata('message', '<div class="alert alert-success"
        role="alert"><a href="" class="close" data-dismiss="alert" aria-
        label="close">&times;</a>Delete succeeded!</div>');
        $this->session->set_flashdata('kode_berhasil', 'suksesModal');
        $this->session->set_flashdata('pesan_berhasil', 'Data guru telah
        dihapus!');
        redirect('guru');
    }

    public function input(){

        $upload_gambar = $_FILES['gambar']['name'];
        if ($upload_gambar) {

            $config['upload_path']      = './assets/img/gambar/';
            $config['allowed_types']     = 'jpeg|jpg|png';

            $this->load->library('upload', $config);

            if ($this->upload->do_upload('gambar')){

                $config['image_library'] = 'gd2';
                $config['source_image']  = './assets/img/gambar/'.$this->upload-
                >data('file_name');
                $config['create_thumb']  = FALSE;
                $config['maintain_ratio'] = FALSE;
                $config['quality']       = '50%';
                $config['width']         = 380;
                $config['height']        = 500;
            }
        }
    }
}

```

```

        $config['new_image']      = './assets/img/gambar/'.$this->upload-
>data('file_name');
        $this->load->library('image_lib', $config);
        $this->image_lib->resize();

        $data = [
            'nip' => htmlspecialchars($this->input->post('nip', true)),
            'nama' => htmlspecialchars($this->input->post('nama', true)),
            'alamat' => htmlspecialchars($this->input->post('alamat', true)),
            'jen_kel' => htmlspecialchars($this->input->post('jen_kel',
true)),
            'tempat_lahir' => htmlspecialchars($this->input-
>post('tempat_lahir', true)),
            'tanggal_lahir' => htmlspecialchars($this->input-
>post('tanggal_lahir', true)),
            'foto' => htmlspecialchars($this->upload->data('file_name',
true)),
            'pass_guru' => htmlspecialchars($this->input->post('nama',
true))
        ];

        $this->db->insert('tb_guru', $data);
        $this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a> New Data added!</div>');
        $this->session->set_flashdata('kode_berhasil', 'suksesModal');
        $this->session->set_flashdata('pesan_berhasil', 'Data guru telah
ditambahkan!');
        redirect('guru');
    }
    else {

        $this->session->set_flashdata('message', '<div class="alert alert-
danger" role="alert">' . $this->upload->display_errors() . '</div>');
        $this->session->set_flashdata('kode_gagal', 'gagalModal');
        $this->session->set_flashdata('pesan_gagal', 'Gagal unggah Foto,
Pastikan jenis file PNG/JPG/JPEG!');
        redirect('guru');
    }

```

```

    }
}

public function edit($id){

    $data['title'] = 'Kelola Data';
    $data['user'] = $this->db->get_where('tb_admin', ['username' => $this->session->userdata('username')])>row_array();

    $data['guru_data'] = $this->db->get_where('tb_guru', ['id_guru' => $id])>row_array();

    $this->load->view('templates/header', $data);
    $this->load->view('templates/sidebar', $data);
    $this->load->view('templates/topbar', $data);
    $this->load->view('guru/edit', $data);
    $this->load->view('templates/footer');
}

public function edit_proses(){

    $upload_gambar = $_FILES['gambar']['name'];

    if ($upload_gambar){

        $config['upload_path']      = './assets/img/gambar/';
        $config['allowed_types']    = 'jpeg|jpg|png';

        $this->load->library('upload', $config);

        if ($this->upload->do_upload('gambar')){

            $config['image_library'] = 'gd2';
            $config['source_image']  = './assets/img/gambar/'.$this->upload->data('file_name');
            $config['create_thumb']  = FALSE;
            $config['maintain_ratio'] = FALSE;
            $config['quality']       = '50%';
            $config['width']        = 380;

```



```

        $config['height']      = 500;
        $config['new_image']   = './assets/img/gambar/'. $this->upload-
>data('file_name');
        $this->load->library('image_lib', $config);
        $this->image_lib->resize();

        $old_image = $this->input->post('gambar_lama');
        $new_image = $this->upload->data('file_name');

        unlink(FCPATH . 'assets/img/gambar/' . $old_image);

        $this->db->set('foto', $new_image);

    }else {

        $this->session->set_flashdata('message', '<div class="alert alert-
danger" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>' . $this->upload->display_errors() . '</div>');
        $this->session->set_flashdata('kode_gagal', 'gagalModal');
        $this->session->set_flashdata('pesan_gagal', 'Gagal unggah Foto,
Pastikan jenis file PNG/JPG/JPEG!');
        redirect('guru');
    }

}

$id_guru = $this->input->post('id_guru');
$nama = $this->input->post('nama');
$nip = $this->input->post('nip');
$alamat = $this->input->post('alamat');
$jen_kel = $this->input->post('jen_kel');
$tempat_lahir = $this->input->post('tempat_lahir');
$tanggal_lahir = $this->input->post('tanggal_lahir');
$this->db->set('nama', $nama);
$this->db->set('nip', $nip);
$this->db->set('alamat', $alamat);
$this->db->set('jen_kel', $jen_kel);
$this->db->set('tempat_lahir', $tempat_lahir);
$this->db->set('tanggal_lahir', $tanggal_lahir);
$this->db->where('id_guru', $id_guru);

```

```
$this->db->update('tb_guru');
```

```
$this->session->set_flashdata('message', '<div class="alert alert-success"
role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Update succeeded!</div>');
```

```
$this->session->set_flashdata('kode_berhasil', 'suksesModal');
```

```
$this->session->set_flashdata('pesan_berhasil', 'Data guru telah
diperbaharui!');
```

```
redirect('guru');
```

```
}
```

```
}
```

5. Jadwal.php

```
<?php
```

```
defined('BASEPATH') OR exit('No direct script access allowed');
```

```
class Jadwal extends CI_Controller
```

```
{
```

```
public function __construct()
```

```
{
```

```
parent::__construct();
```

```
if (!$this->session->userdata('username')) {
```

```
    redirect('auth');
```

```
}
```

```
$this->load->library('Ciqrcode');
```

```
}
```

```
public function index()
```

```
{
```

```
$data['title'] = 'Jadwal Mengajar';
```

```
$data['user'] = $this->db->get_where('tb_admin', ['username' =>
```

```
$this->session->userdata('username')])->row_array();
```

```
$this->db->join('tb_kelas', 'tb_kelas.id_kelas=tb_jadwal.id_kelas');
```

```
$this->db->join('tb_mapel',
```

```
'tb_mapel.id_mapel=tb_jadwal.id_mapel');
```

```

        $this->db->join('tb_pengampuh',
'tb_pengampuh.id_mapel=tb_jadwal.id_mapel');
        $this->db->join('tb_guru',
'tb_guru.id_guru=tb_pengampuh.id_guru');
        $data['jadwal'] = $this->db->get('tb_jadwal')->result_array();

        $data['kelas'] = $this->db->get('tb_kelas')->result_array();
        $data['mapel'] = $this->db->get('tb_mapel')->result_array();

        $this->load->view('templates/header', $data);
        $this->load->view('templates/sidebar', $data);
        $this->load->view('templates/topbar', $data);
        $this->load->view('jadwal/index', $data);
        $this->load->view('templates/footer');

    }

    public function input(){

        $data = [
            'id_kelas' => htmlspecialchars($this->input-
>post('nama_kelas', true)),
            'hari_masuk' => htmlspecialchars($this->input-
>post('hari_masuk', true)),
            'jam_masuk' => htmlspecialchars($this->input-
>post('jam_masuk', true)),
            'jam_selesai' => htmlspecialchars($this->input-
>post('jam_selesai', true)),
            'id_mapel' => htmlspecialchars($this->input-
>post('nama_mapel', true))
        ];

        $this->db->insert('tb_jadwal', $data);
        $this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Jadwal ditambahkan!</div>');
        $this->session->set_flashdata('kode_berhasil', 'suksesModal');
        $this->session->set_flashdata('pesan_berhasil', 'Data jadwal telah
ditambahkan!');
        redirect('jadwal');
    }

```

```

    }

    public function hapus($id){
        $this->db->where('id_jadwal', $id);
        $this->db->delete('tb_jadwal');
        $this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"> Delete succeeded!</div>');
        redirect('jadwal');
    }

    public function edit($id){

        $data['title'] = 'Jadwal Mengajar';
        $data['user'] = $this->db->get_where('tb_admin', ['username' =>
$this->session->userdata('username')])->row_array();

        $ambil_kelas = $this->db->get_where('tb_jadwal', ['id_jadwal' =>
$id])->row_array();
        $id_kelas = $ambil_kelas['id_kelas'];
        $ambil_mapel = $this->db->get_where('tb_jadwal', ['id_jadwal' =>
$id])->row_array();
        $id_mapel = $ambil_kelas['id_mapel'];
        $data['jadwal_data'] = $this->db->get_where('tb_jadwal',
['id_jadwal' => $id])->row_array();
        $data['kelas_data'] = $this->db->get_where('tb_kelas', ['id_kelas'
=> $id_kelas])->row_array();
        $data['mapel_data'] = $this->db->get_where('tb_mapel',
['id_mapel' => $id_mapel])->row_array();
        $data['kelas'] = $this->db->get('tb_kelas')->result_array();
        $data['mapel'] = $this->db->get('tb_mapel')->result_array();
        $this->load->view('templates/header', $data);
        $this->load->view('templates/sidebar', $data);
        $this->load->view('templates/topbar', $data);
        $this->load->view('jadwal/edit', $data);
        $this->load->view('templates/footer');
    }

    public function edit_proses(){
        $id_jadwal = $this->input->post('id_jadwal');
        $nama_mapel = $this->input->post('nama_mapel');

```

```

$nama_kelas = $this->input->post('nama_kelas');
$hari_masuk = $this->input->post('hari_masuk');
$jam_masuk = $this->input->post('jam_masuk');
$jam_selesai = $this->input->post('jam_selesai');
$this->db->set('hari_masuk', $hari_masuk);
$this->db->set('jam_masuk', $jam_masuk);
$this->db->set('jam_selesai', $jam_selesai);
$this->db->set('id_mapel', $nama_mapel);
$this->db->set('id_kelas', $nama_kelas);
$this->db->where('id_jadwal', $id_jadwal);
$this->db->update('tb_jadwal');
$this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Update jadwal berhasil!</div>');
$this->session->set_flashdata('kode_berhasil', 'suksesModal');
$this->session->set_flashdata('pesan_berhasil', 'Data jadwal telah
diperbaharui!');
        redirect('jadwal');
    }
}

```

6. Kelas.php

```

<?php
defined('BASEPATH') OR exit('No direct script access allowed');

class Kelas extends CI_Controller
{

    public function __construct()
    {
        parent::__construct();
        if (!$this->session->userdata('username')) {
            redirect('auth');
        }
    }

    public function index()
    {
        $data['title'] = 'Kelola Data';
        $data['user'] = $this->db->get_where('tb_admin', ['username' =>
$this->session->userdata('username')])->row_array();
    }
}

```

```

$data['kelas'] = $this->db->get('tb_kelas')->result_array();

$this->load->view('templates/header', $data);
$this->load->view('templates/sidebar', $data);
$this->load->view('templates/topbar', $data);
$this->load->view('kelas/index', $data);
$this->load->view('templates/footer');
}
public function input(){
    $kode_kelas = $this->input->post('kode_kelas');
    $cek = $this->db->get_where('tb_kelas', ['kode_kelas' =>
$kode_kelas])->num_rows();
    if ($cek > 0) {
        $this->session->set_flashdata('message', '<div class="alert
alert-danger" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Maaf, kelas Sudah Ada!</div>');
        $this->session->set_flashdata('kode_gagal', 'gagalModal');
        $this->session->set_flashdata('pesan_gagal', 'Kode kelas
sudah ada!');
        redirect('kelas');
    }else{
        $data = [
            'kode_kelas' => htmlspecialchars($kode_kelas),
            'nama_kelas' => htmlspecialchars($this->input-
>post('nama_kelas', true))
        ];

        $this->db->insert('tb_kelas', $data);
        $this->session->set_flashdata('message', '<div class="alert
alert-success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Data kelas ditambahkan!</div>');
        $this->session->set_flashdata('kode_berhasil',
'suksesModal');
        $this->session->set_flashdata('pesan_berhasil', 'Data kelas
telah ditambahkan!');
        redirect('kelas');
    }
}
public function hapus($id){

```

```

        $this->db->where('id_kelas', $id);
        $this->db->delete('tb_kelas');
        $this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a> Delete succeeded!</div>');
        $this->session->set_flashdata('kode_berhasil', 'suksesModal');
        $this->session->set_flashdata('pesan_berhasil', 'Data kelas telah
dihapus!');
        redirect('kelas');
    }
}

```

7. Mapel.php

```

<?php
defined('BASEPATH') OR exit('No direct script access allowed');
class Mapel extends CI_Controller
{
    public function __construct()
    {
        parent::__construct();
        if (!$this->session->userdata('username')) {
            redirect('auth');
        }
    }

    public function index()
    {
        $data['title'] = 'Kelola Data';
        $data['user'] = $this->db->get_where('tb_admin', ['username' =>
$this->session->userdata('username')])->row_array();
        $data['mapel'] = $this->db->get('tb_mapel')->result_array();
        $this->load->view('templates/header', $data);
        $this->load->view('templates/sidebar', $data);
        $this->load->view('templates/topbar', $data);
        $this->load->view('mapel/index', $data);
        $this->load->view('templates/footer');
    }

    public function input(){
        $kode_mapel = $this->input->post('kode_mapel');
        $cek = $this->db->get_where('tb_mapel', ['kode_mapel' =>
$kode_mapel])->num_rows();
    }
}

```

```

        if ($cek > 0) {
            $this->session->set_flashdata('message', '<div class="alert
alert-danger" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Maaf, Mapel Sudah Ada!</div>');
            $this->session->set_flashdata('kode_gagal', 'gagalModal');
            $this->session->set_flashdata('pesan_gagal', 'Kode mapel
sudah ada!');

            redirect('mapel');
        }else{
            $data = [
                'kode_mapel' => htmlspecialchars($kode_mapel),
                'nama_mapel' => htmlspecialchars($this->input-
>post('nama_mapel', true))
            ];

            $this->db->insert('tb_mapel', $data);
            $this->session->set_flashdata('message', '<div class="alert
alert-success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Data mapel ditambahkan!</div>');
            $this->session->set_flashdata('kode_berhasil',
'suksesModal');
            $this->session->set_flashdata('pesan_berhasil', 'Data mapel
telah ditambahkan!');
            redirect('mapel');
        }
    }

    public function hapus($id){
        $this->db->where('id_mapel', $id);
        $this->db->delete('tb_mapel');
        $this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a> Delete succeeded!</div>');
        $this->session->set_flashdata('kode_berhasil', 'suksesModal');
        $this->session->set_flashdata('pesan_berhasil', 'Data mapel telah
dihapus!');
        redirect('mapel');
    }
}

```

8. Pass.php
<?php


```

defined('BASEPATH') OR exit('No direct script access allowed');
class Pass extends CI_Controller
{
    public function __construct()
    {
        parent::__construct();
        if (!$this->session->userdata('username')) {
            redirect('auth');
        }
    }
    public function index()
    {
        $data['title'] = 'My Profile';
        $data['user'] = $this->db->get_where('tb_admin', ['username' =>
$this->session->userdata('username')])->row_array();
        $this->load->view('templates/header', $data);
        $this->load->view('templates/sidebar', $data);
        $this->load->view('templates/topbar', $data);
        $this->load->view('pass/index', $data);
        $this->load->view('templates/footer');
    }
    public function edit_password(){
        $id = $this->input->post('id');
        $new_pass = $this->input->post('password_baru');
        $wkt = time();
        $pass = password_hash($new_pass, PASSWORD_DEFAULT);
        $this->db->set('password', $pass);
        $this->db->where('id', $id);
        $this->db->update('tb_admin');
        $this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"> Password has changed!</div>');
        $this->session->set_flashdata('kode_berhasil', 'suksesModal');
        $this->session->set_flashdata('pesan_berhasil', 'Password anda
telah diperbaharui!');
        redirect('pass');
    }
}

```

9. Qrcode.php

```

<?php
defined('BASEPATH') OR exit('No direct script access allowed');

```

```

class Qrkode extends CI_Controller
{
    public function __construct()
    {
        parent::__construct();
        if (!$this->session->userdata('username')) {
            redirect('auth');
        }
        $this->load->library('Ciqrcode');
    }
    public function index()
    {
        $data['title'] = 'QRCode Absen';
        $data['user'] = $this->db->get_where('tb_admin', ['username' =>
$this->session->userdata('username')])->row_array();
        $data['qrkode'] = $this->db->get('tb_qrcode')->result_array();
        $this->load->view('templates/header', $data);
        $this->load->view('templates/sidebar', $data);
        $this->load->view('templates/topbar', $data);
        $this->load->view('qrkode/index', $data);
        $this->load->view('templates/footer');
    }
    public function input(){
        $cek = $this->db->get('tb_qrcode')->num_rows();
        if ($cek > 0) {
            $this->session->set_flashdata('message', '<div class="alert
alert-danger" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Hapus QRCode yang ada terlebih dahulu!</div>');
            $this->session->set_flashdata('kode_gagal', 'gagalModal');
            $this->session->set_flashdata('pesan_gagal', 'Maaf,
Pembuatan QRCode untuk Absensi hanya dibatasi 1 saja!');
            redirect('qrkode');
        }else {
            function random_word($id = 10){
                $pool = '1234567890abcdefghijklmnopqrstuvwxyz';
                $word = "";
                for ($i = 0; $i < $id; $i++){
                    $word .= substr($pool, mt_rand(0,
strlen($pool) - 1), 1);
                }
            }
        }
    }
}

```

```

        return $word;
    }
    $acak_kode = random_word(5).time();
    $enkrip_sha256 = hash("sha256", $acak_kode);
    $hash_bcrypt = password_hash($enkrip_sha256,
PASSWORD_DEFAULT);
    $data = [
        'kode_absen' => htmlspecialchars($hash_bcrypt),
        'created' => time()];
    $this->db->insert('tb_qrcode', $data);
    $this->session->set_flashdata('message', '<div class="alert
alert-success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>QRCode berhasil dibuat!</div>');
    $this->session->set_flashdata('kode_berhasil', 'suksesModal');
    $this->session->set_flashdata('pesan_berhasil', 'QRCode baru telah
ditambahkan!');
    redirect('qrkode');
    }
}
public function hapus($id){
    $this->db->where('id_qrcode', $id);
    $this->db->delete('tb_qrcode');
    $this->session->set_flashdata('message', '<div class="alert alert-
success" role="alert"><a href="" class="close" data-dismiss="alert" aria-
label="close">&times;</a>Delete succeeded!</div>');
    $this->session->set_flashdata('kode_berhasil', 'suksesModal');
    $this->session->set_flashdata('pesan_berhasil', 'Data QRCode telah
dihapus!');
    redirect('qrkode');
}
public function QRcode()
{
    $kode = $this->input->post('kode_absen');
    QRcode::png(
        $kode,
        $outfile = false,
        $level = QR_ECLEVEL_H,
        $size = 12,
        $margin = 2
    ); }}

```



PEMERINTAH KABUPATEN BOLAANG MOGNONDOW
DINAS PENDIDIKAN
SMP NEGERI 4 LOLAYAN
JL. RAYA MOPUSI KECAMATAN LOLAYAN KODE POS 95771

SURAT KETERANGAN

Nomor : 127 / C.03 / SMP 4 Lolayan / 2021

Yang bertanda tangan di bawah ini :

Nama : RAHMAN LAOH, S.Pd., MPd
NIP : 19770418 200801 1 008
Pangkat / Gol. : Pembina / IV A
Jabatan : Kepala SMP Negeri 4 Lolayan

Menerangkan dengan benar bahwa Mahasiswa tersebut di bawah ini telah melakukan penelitian di SMP Negeri 4 Lolayan pada Tahun Pelajaran 2021 / 2022.

Nama : ARGRIYANTO ASIKING
Tempat / Tgl. Lahir : Mopusi, 19 Juli 1999
Nim : T3117147
Alamat : Desa Mopusi Kecamatan Lolayan

Demikian Surat keterangan ini dibuat dengan benar untuk digunakan sebagaimana mestinya.

Dikeluarkan di : Mopusi
Pada tanggal : 1 Maret 2021





KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
FAKULTAS ILMU KOMPUTER
UPT. PERPUSTAKAAN FAKULTAS
SK. MENDIKNAS RI NO. 84/D/0/2001
Jl. Achmad Nadjamuddin No.17 Telp(0435) 829975 Fax. (0435) 829976 Gorontalo

SURAT KETERANGAN BEBAS PUSTAKA

No : 005/Perpustakaan-Fikom/XII/2021

Perpustakaan Fakultas Ilmu Komputer (FIKOM) Universitas Ichsan Gorontalo dengan ini menerangkan bahwa :

Nama Anggota : Agriyanto Asiking
No. Induk : T3117147
No. Anggota : M202175

Terhitung mulai hari, tanggal : Senin, 06 Desember 2021, dinyatakan telah bebas pinjam buku dan koleksi perpustakaan lainnya.

Demikian keterangan ini di buat untuk di pergunakan sebagaimana mestinya.

Gorontalo, 06 Desember 2021

Mengetahui,
Kepala Perpustakaan



Apriyanto Alhamad, M.Kom

NIDN : 0924048601



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN
**UNIVERSITAS ICHSAN
(UNISAN) GORONTALO**

SURAT KEPUTUSAN MENDIKNAS RI NOMOR 84/D/O/2001
Jl. Achmad Nadjamuddin No. 17 Telp (0435) 829975 Fax (0435) 829976 Gorontalo

SURAT REKOMENDASI BEBAS PLAGIASI

No. 1023/UNISAN-G/S-BP/XII/2021

Yang bertanda tangan di bawah ini:

Nama : Sunarto Taliki, M.Kom
NIDN : 0906058301
Unit Kerja : Pustikom, Universitas Ichsan Gorontalo

Dengan ini Menyatakan bahwa :

Nama Mahasiswa : AGRIYANTO ASIKING
NIM : T3117147
Program Studi : Teknik Informatika (S1)
Fakultas : Fakultas Ilmu Komputer
Judul Skripsi : Quick Response Code Absensi guru menggunakan
secure hashing algoritma (SHA)

Sesuai dengan hasil pengecekan tingkat kemiripan skripsi melalui aplikasi Turnitin untuk judul skripsi di atas diperoleh hasil Similarity sebesar 29%, berdasarkan SK Rektor No. 237/UNISAN-G/SK/IX/2019 tentang Panduan Pencegahan dan Penanggulangan Plagiarisme, bahwa batas kemiripan skripsi maksimal 35% dan sesuai dengan Surat Pernyataan dari kedua Pembimbing yang bersangkutan menyatakan bahwa isi softcopy skripsi yang diolah di Turnitin SAMA ISINYA dengan Skripsi Aslinya serta format penulisannya sudah sesuai dengan Buku Panduan Penulisan Skripsi, untuk itu skripsi tersebut di atas dinyatakan BEBAS PLAGIASI dan layak untuk diujikan.

Demikian surat rekomendasi ini dibuat untuk digunakan sebagaimana mestinya.

Gorontalo, 04 Desember 2021

Tim Verifikasi,



Sunarto Taliki, M.Kom
NIDN. 0906058301

Tembusan :

1. Dekan
2. Ketua Program Studi
3. Pembimbing I dan Pembimbing II
4. Yang bersangkutan
5. Arsip

T3117147 AGRYANTO ASKING

QUICK RESPONSE CODE ABSENSI GURU MENGGUNAKAN SEC...

Sources Overview

29%

OVERALL SIMILARITY

| | | |
|----|------------------------------|-----|
| 1 | njs.trigonadharma.ac.id | 8% |
| 2 | repository.bai.ac.id | 2% |
| 3 | diglib.unila.ac.id | 2% |
| 4 | paetebn.com | 2% |
| 5 | ejournal.amikunai.ac.id | 1% |
| 6 | harviacode.com | 1% |
| 7 | www.scribd.com | <1% |
| 8 | media.neliti.com | <1% |
| 9 | es.scribd.com | <1% |
| 10 | nitamanurlingga.blogspot.com | <1% |
| 11 | widati.raharja.info | <1% |
| 12 | eprints.uny.ac.id | <1% |
| 13 | stmk-ichean.ac.id | <1% |
| 14 | ejournal.ugitatan.ac.id | <1% |
| 15 | meliantan11.blogspot.com | <1% |
| 16 | 48khadijah2215.wordpress.com | <1% |

RIWAYAT HIDUP



Nama : Agriyanto Asiking
Nim : T3117147
Tempat, Tanggal Lahir : Mopusi, 19 Juli 1999
Agama : Islam
Email : Agri@gmail.com

Riwayat Pendidikan :

Tahun 2011, Menyelesaikan Pendidikan di Sekolah Dasar Negeri 1 Mopusi
Kecamatan Lolayan, Bolaang Mongondow

Tahun 2014, Menyelesaikan di Sekolah Menengah Pertama di SMP Negeri
Lolayan, Kecamatan Lolayan, Bolaang Mongondow

Tahun 2017, Menyelesaikan Sekolah Menengah Kejuruan di SMK
Cokroaminoto Kotamubagu, Sulawesi Utara

Tahun 2017, Mendaftar dan Diterima Menjadi Mahasiswa di Fakultas Ilmu
Komputer

Jurusan Teknik Informatika Universitas Ichsan Gorontalo.