IMPLEMENTASI *SECURE HASH ALGORITHM*-256, *RIVEST SHAMIR ADLEMAN*, DAN *QUICK RESPONSE CODE* PADA *DIGITAL SIGNATURE* UNTUK MENENTUKAN KEABSAHAN DOKUMEN PROPOSAL DAN SURAT

Lestari Aghnia Rahma
Fakultas Teknik
Program Studi Informatika
Universitas Langlangbuana
lestariagnrhm@gmail.com

Aisyah Nuraeni
Fakultas Teknik
Program Studi Informatika
Universitas Langlangbuana
aisyahnuraeni@unla.ac.id

Hadi Prasetyo Utomo
Fakultas Teknik
Program Studi Informatika
Universitas Langlangbuana
students.hpu@gmail.com

Abstrak - Penandatanganan dokumen proposal dan surat merupakan suatu hal yang sering digunakan di Universitas Langlangbuana khususnya di Lembaga Keluarga Mahasiswa Fakultas Teknik. Namun pada penggunaannya banyak dokumen yang disahkan menggunakan tanda tangan manual hasil *scan* dan mudah untuk di*copy paste*, sehingga sering dipertanyakan keabsahannya. Masalah lain yaitu jika pihak yang harus melakukan pengesahan tidak berada bersamaan di kampus, sehingga permohonan tanda tangan ini dapat menghabiskan waktu yang lama. Dengan perkembangan sistem kriptografi terdapat fasilitas tanda tangan digital yang dapat memberikan layanan keamanan sehingga tidak akan terjadi pemalsuan tanda tangan. Berdasarkan uraian tersebut maka dibuatlah aplikasi untuk tanda tangan digital yang dibangun dengan menerapkan fungsi *hashing* yaitu *Secure Hash Algorithm (SHA)*-256 dan algoritma asimetris yaitu *Rivest Shamir Adleman (RSA)*, serta penggunaan *Quick Response Code (QR-Code)* sebagai penentuan keabsahannya. Penelitian ini juga menggunakan metode rekayasa *forward engineering* dan metode pengembangan sistem yaitu model *waterfall.*

Kata kunci - *Pemalsuan, Digital Signature, Secure Hash Algorithm (SHA)-256, Rivest Shamir Adleman (RSA), dan Quick Response Code (QR-Code).*

1. PENDAHULUAN (*HEADING 1*)

Bagaikan dua sisi mata uang yang berbeda, teknologi memberikan kemudahan dan kemajuan peradaban manusia, namun disisi lain meningkat juga kejahatan yang disebabkan tindak penyalahgunaan teknologi tersebut. Salah satu contoh kasus dikemukakan oleh Mardheana (2012) "Notaris di Kabupaten Sleman yang telah terbukti bersalah melakukan perbuatan pidana yaitu membuat minuta akta dengan memalsukan tandantangan penghadap. Hal ini di perkuat dengan adanya bukti dokumen Berita Acara Pemeriksaan Laboratoris Kriminalistik Nomor Lab. 416/DTF/IV/2011 tanggal 03 Mei 2011 yang ditandatangani oleh Yayuk Murti Rahayu Bsc, Drs. Moh. Arief Buudiarto, dan Budi Santoso, S.Si. yang menyimpulkan bahwa tanda tangan Ir. Gregorius Daryanto atau penghadap adalah merupakan tanda tangan berbeda dalam akta surat kuasa jual nomor 51, surat kuasa jual Nomor 52 dan surat perikatan jual beli Nomor 65. Berdasarkan kejadian tersebut notaris Endang Murniati, S.H., dituntut oleh Jaksa Penuntut Umum dengan Pasal 263 ayat 1 dan Pasal 264 ayat 1 Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP) dengan tuduhan pembuatan surat/dokumen palsu".

Di Universitas Langlangbuana terutama pada lembaga di ruang lingkup Fakultas Teknik penggunaan tanda tangan banyak dijumpai pada hal-hal yang berkaitan dengan administrasi. Namun pada penggunaannya banyak dokumen yang disahkan menggunakan tanda tangan manual hasil *scan* dan mudah untuk di*copy paste*, sehingga sering dipertanyakan keabsahan nya. Masalah lain yaitu jika pihak yang harus melakukan pengesahan tidak berada bersamaan di kampus, sehingga permohonan tanda tangan ini dapat menghabiskan waktu yang lama. Hal-hal tersebut menjadi poin permasalahan, maka diperlukan penerapan perubahan konsep

manual menjadi digital agar proses penandatanganan tidak memakan waktu yang lama serta menerapkan pengamanan agar terjaga keabsah dari tanda tangan tersebut.

Banyak teknologi yang dapat digunakan untuk mengurangi kasus tersebut, salah satunya teknologi *Quick Response Code (QR-Code). Quick Response Code (QR-Code)* memiliki kapasitas tinggi dalam penyimpanan data, namun penggunaannya tidak menjamin dalam menjaga keamanan penyimpanan data, sehingga diperlukan mekanisme lain yang dapat membuat data yang ada di dalam *Quick Response Code (QR-Code)* menjadi aman dari penyalahgunaan. Cabang ilmu yang membahas terkait keamanan data tersebut yaitu kriptografi, salah satu pengembangan dari kriptografi adalah *Digital Signature*. *Digital Signature* dapat memberi tanda pada data yang dapat memastikan bahwa data tersebut data yang sebenarnya. *Digital Signature* menggunakan 2 algoritma, pada penelitian ini menggunakan *Secure Hash Algorithm (SHA)*-256 untuk proses *hashing* dan *Rivest Shamir Adleman (RSA)* untuk proses pembangkitan kunci dan proses validasi. Data yang sudah selesai melalui proses *Secure Hash Algorithm (SHA)*-256 dan *Rivest Shamir Adleman (RSA)* menghasilkan kode-kode yang tidak dapat terbaca yang kemudian disimpan dalam *Quick Response Code (QR-Code)*.

Adapun tujuan penelitian ini yaitu menyajikan aplikasi tanda tangan digital yang mempermudah pemohon tanda tangan, pihak-pihak pengesah dan petugas pengecek validasi tanda tangan, kemudian menyajikan aplikasi yang dapat mengamankan tanda tangan digital agar tidak terjadi pemalsuan dan menyajikan aplikasi yang dapat menentukan keabsahan tanda tangan.

2. METODE

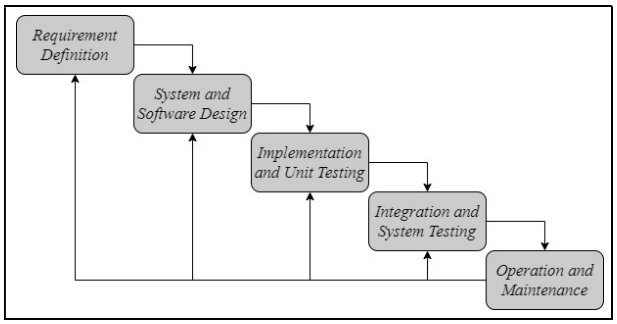
2.1. Metode Penelitian Rekayasa

Metode penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu [1]. Penelitian rekayasa termasuk penelitian perangkat lunak yang merupakan penelitian untuk menerapkan ilmu pengetahuan menjadi suatu rancangan untuk mendapatkan kinerja yang sesuai dengan persyaratan yang ditentukan. [2]. Metode penelitian yang digunakan adalah metode penelitian rekayasa dengan pendekatan *forward engineering*. Tahapan yang dilakukan *forward engineering* yaitu :

1. *Plan*
   Tahapan awal perencanaan terhadap proses penelitian, mendefinisikan tujuan dan ruang lingkup pengembangan kemudian mengidentifikasi masalah-masalah yang ada, dan bisa diselesaikan melalui pengembangan sistem.
2. *Analisis*
   Penguraian dari informasi yang utuh ke dalam bagian-bagian komponennya dengan maksud untuk mengidentifikasikan dan mengevaluasi permasalahan-permasalahan yang ada, sehingga dapat diusulkan perbaikan-perbaikannya.
3. *Design*
   Tahap ini merupakan tahap pemodelan dari hasil analisis yang dikemukakan pada tahap 2, pemodelan berfokus pada perancangan struktur menu, perancangan sistem, perancangan antarmuka, dan perancangan basis data.
4. *Construct*
   Tahap implementasi dari sebuah model yang dibentuk pada tahap ke 3 menjadi bentuk nyata menggunakan *script* kode pemrograman sehingga menghasilkan sistem yang diinginkan.
5. *Applied*
   Merupakan tahap penerapan dari hasil model yang sudah diimplementasikan. Tahap ini merupakan penentuan perubahan sistem dari sistem lama ke sistem baru yang lebih baik. Tahap ini juga merupakan tahap akhir untuk upaya mencapai target yang diinginkan pada tahap 1 hingga tahap 4.

2.2. Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan yaitu metode *waterfall.* Langkah-langkah yang digunakan dijelaskan pada Gambar 1.



Gambar 1. Langkah-langkah Metode *Waterfall* [3]

Langkah-langkah yang dilakukan dalam metode *waterfall*, diantaranya yaitu :

1. *Requirements Analysis and Definition*
   Sistem ini layanan, kendala, dan tujuan ditetapkan oleh konsultasi dengan pengguna sistem. Kemudian ditetapkan secara detail dan melayani sebagai spesifikasi sistem.
2. *System and Software Design*

Proses desain sistem mengalokasikan membutuhkan perangkat keras atau perangkat lunak sistem dengan membentuk sistem secara keseluruhan arsitektur. Desain perangkat lunak melibatkan identifikasi dan menggambarkan abstraksi sistem perangkat lunak.

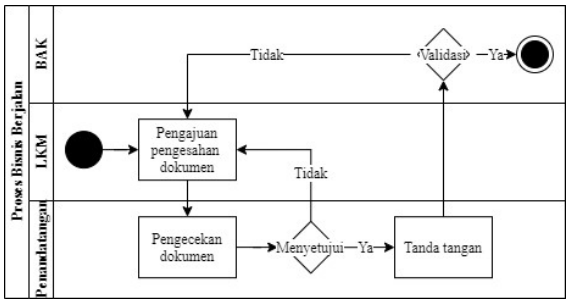
3. *Implementation and Unit Testing*
   Pada tahap ini desain perangkat lunak adalah sebagai seperangkat program atau unit program. Unit pengujian melibatkan verifikasi bahwa setiap unit memenuhi spesifikasinya.
4. *Integration and System Testing*
   Unit program individu atau program diintegrasikan dan diuji sebagai sistem yang lengkap untuk memastikan bahwa perangkat lunak persyaratan telah terpenuhi. Setelah pengujian sistem perangkat lunak disampaikan kepada pelanggan.
5. *Operation and Maintenance* biasanya (meskipun tidak selalu)
   Merupakan fase terpanjang, sistem terinstal dan dimasukkan ke dalam penggunaan praktis.

3. HASIL DAN DISKUSI

3.1. Analisa Proses Bisnis

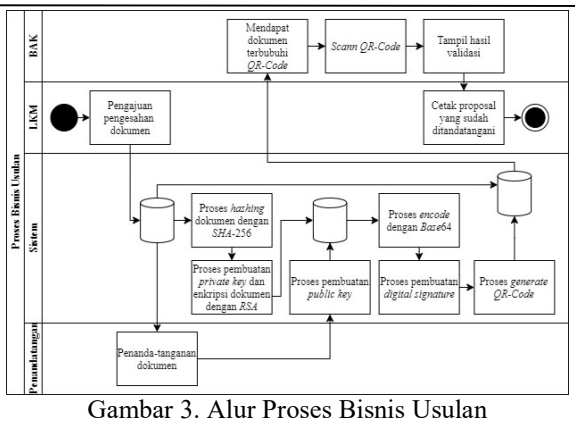
Tahap yang dilakukan untuk mengetahui urutan pelaksanaan dalam suatu kegiatan yang bertujuan untuk mendapatkan keuntungan dengan menggunakan berbagai sumber daya.

1. Proses Bisnis Berjalan



Gambar 2. Alur Proses Bisnis Berjalan

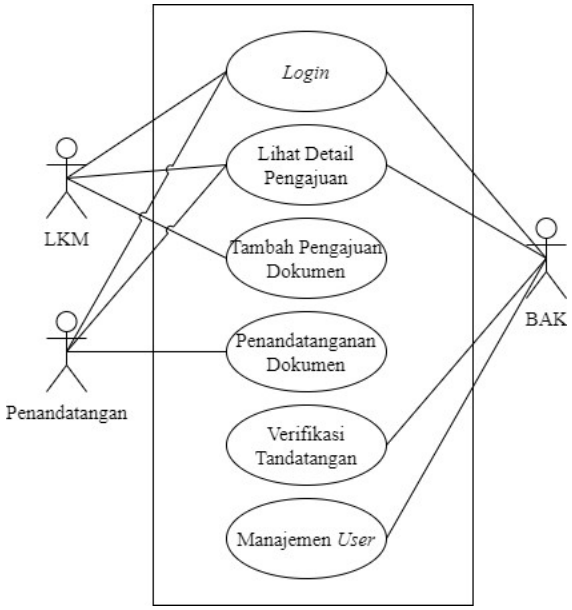
2. Proses Bisnis Usulan



Gambar 3. Alur Proses Bisnis Usulan

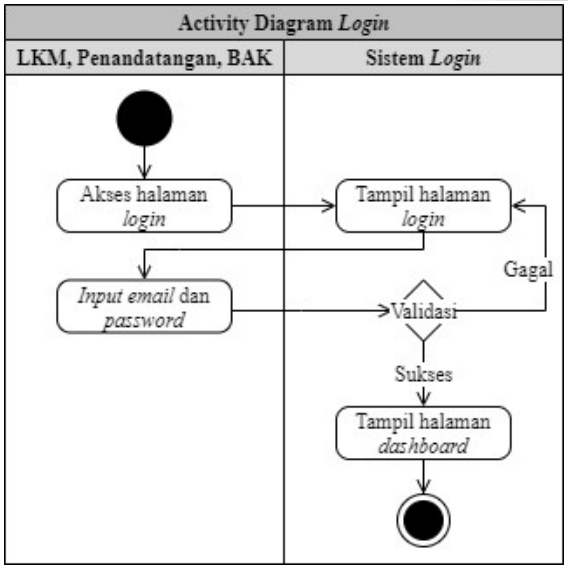
3.2. Perancangan Sistem

1. Pemodelan *Use Case* Diagram

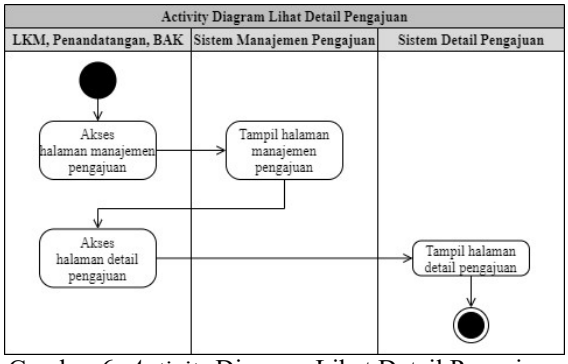


Gambar 4. *Use Case* Diagram

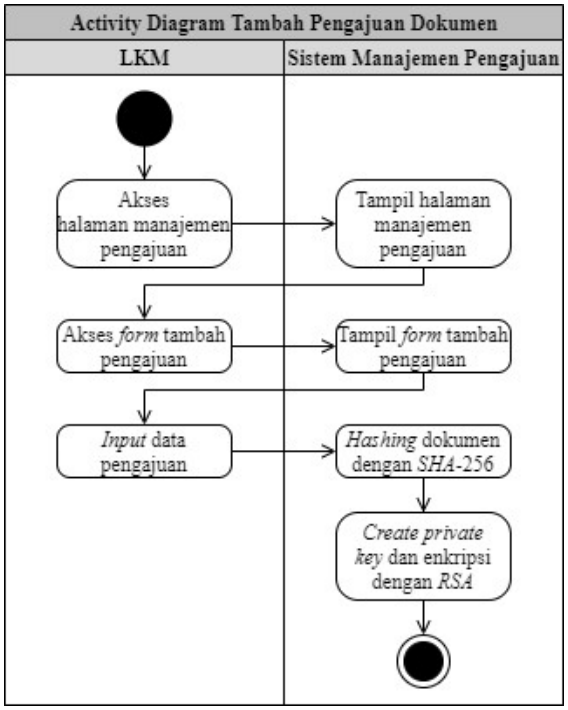
2. Pemodelan *Activity* Diagram



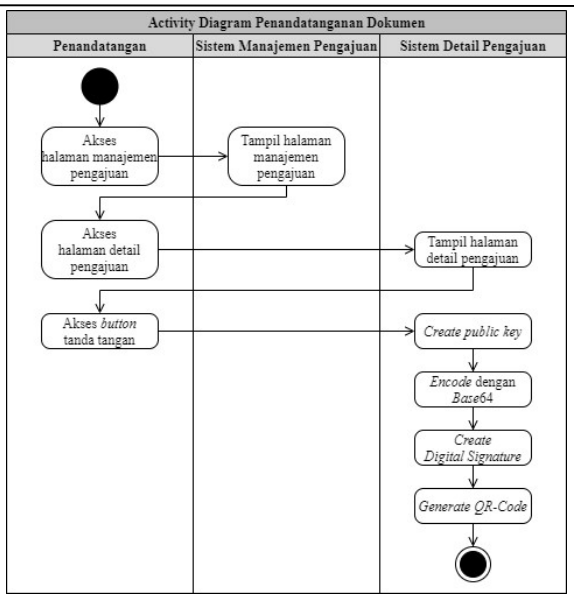
Gambar 5. *Activity* Diagram *Login*



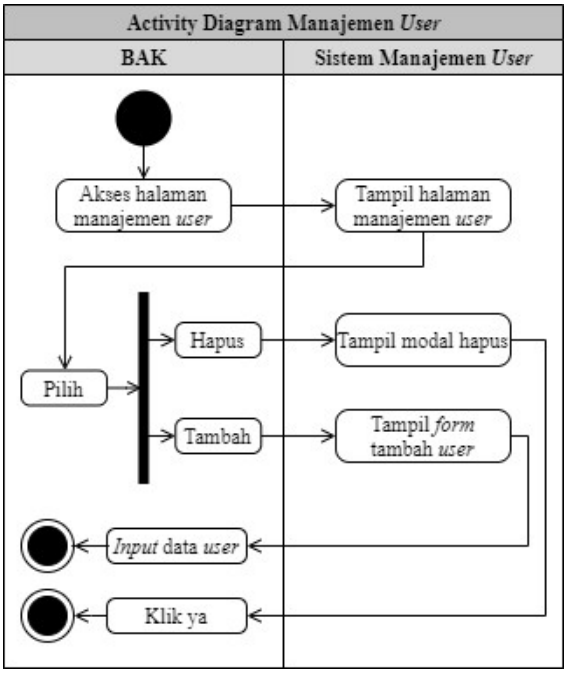
Gambar 6. *Activity* Diagram Lihat Detail Pengajuan



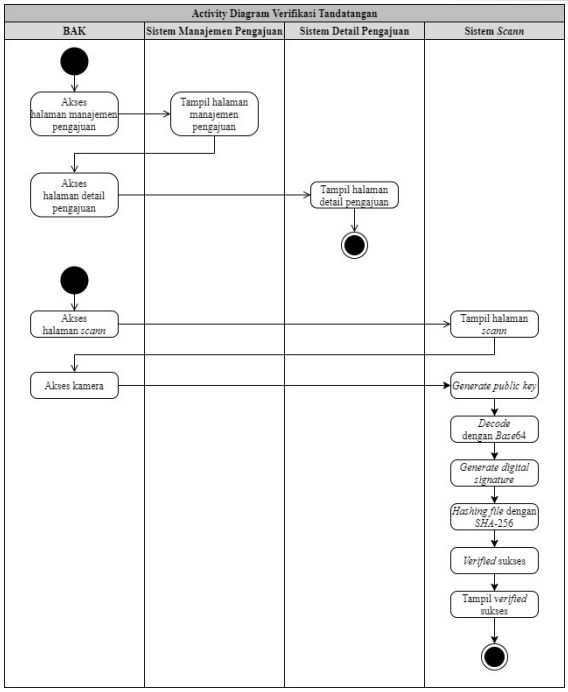
Gambar 7. *Activity* Diagram Tambah Pengajuan Dokumen



Gambar 8. *Activity* Diagram Tambah Penandatanganan Dokumen

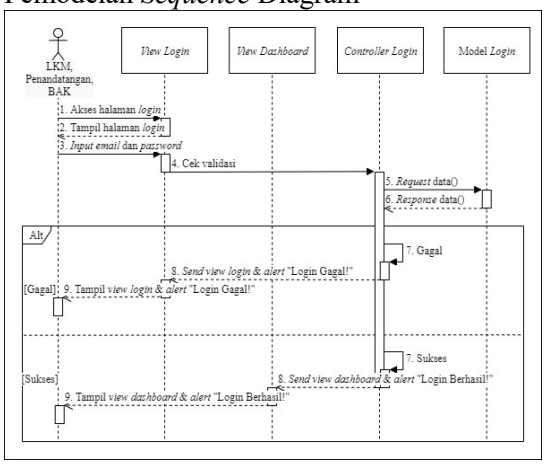


Gambar 9. *Activity* Diagram Manajemen *User*

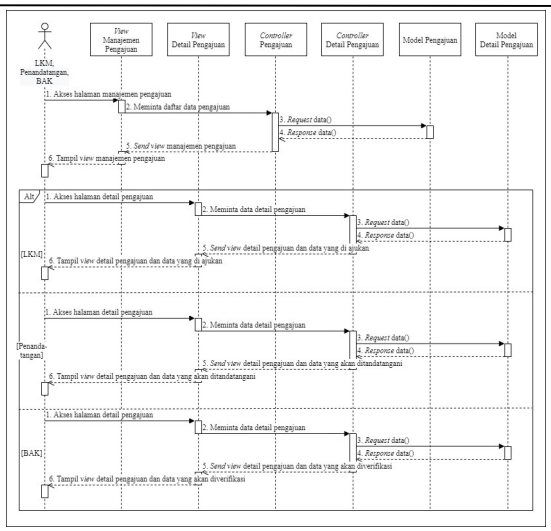


Gambar 10. *Activity* Diagram Verifikasi Tandatangan

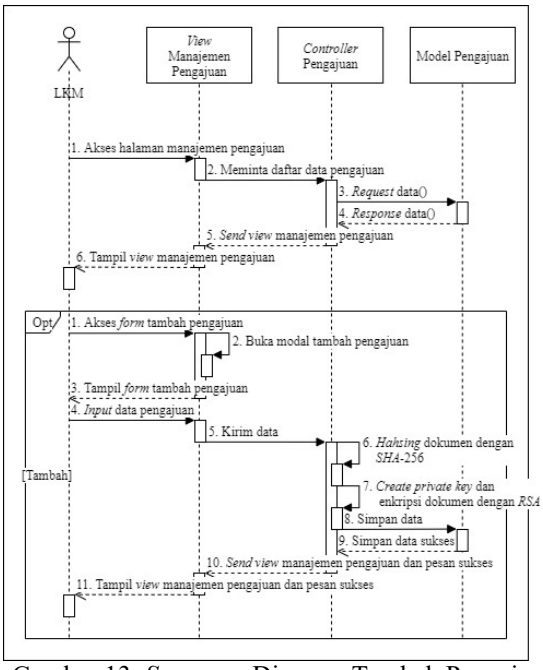
3. Pemodelan *Sequence* Diagram



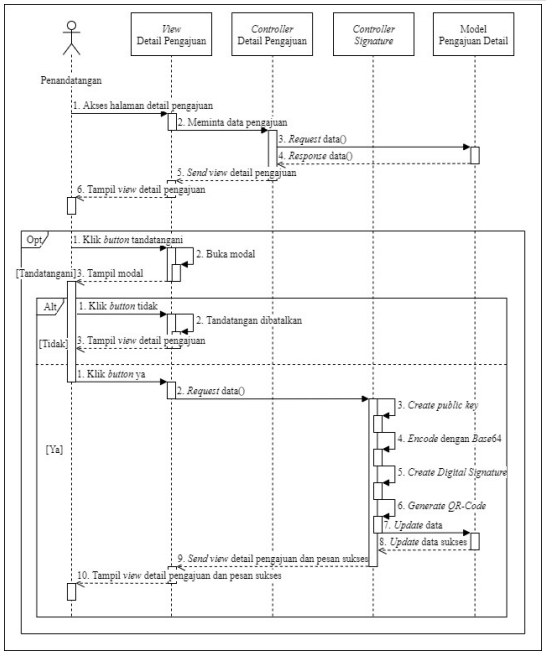
Gambar 11. *Sequence* Diagram *Login*



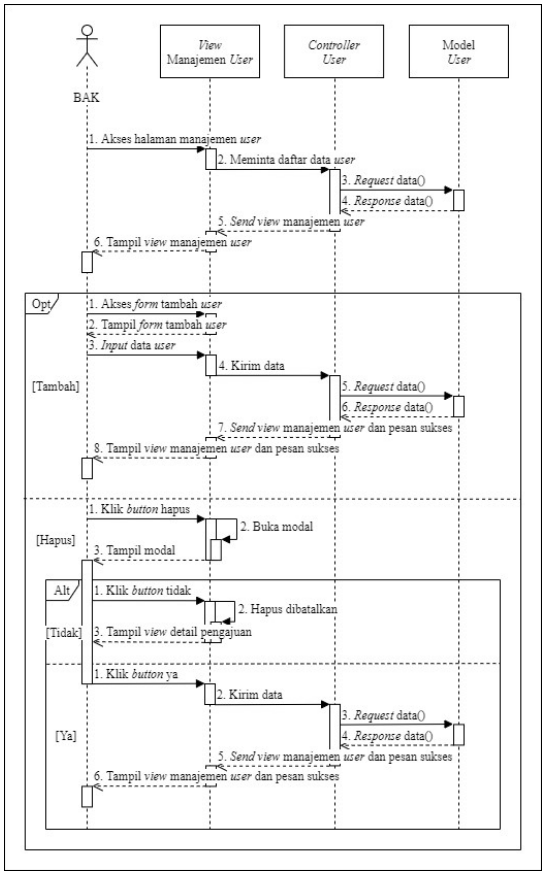
Gambar 12. *Sequence* Diagram Lihat Detail Pengajuan



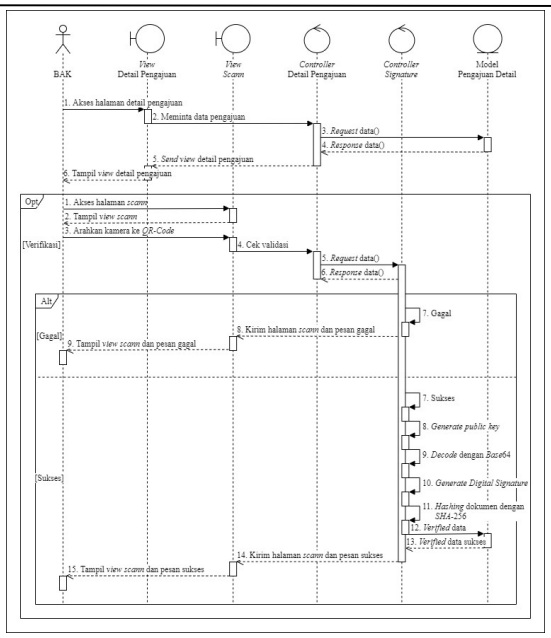
Gambar 13. *Sequence* Diagram Tambah Pengajuan Dokumen



Gambar 14. *Sequence* Diagram Penandatanganan Dokumen

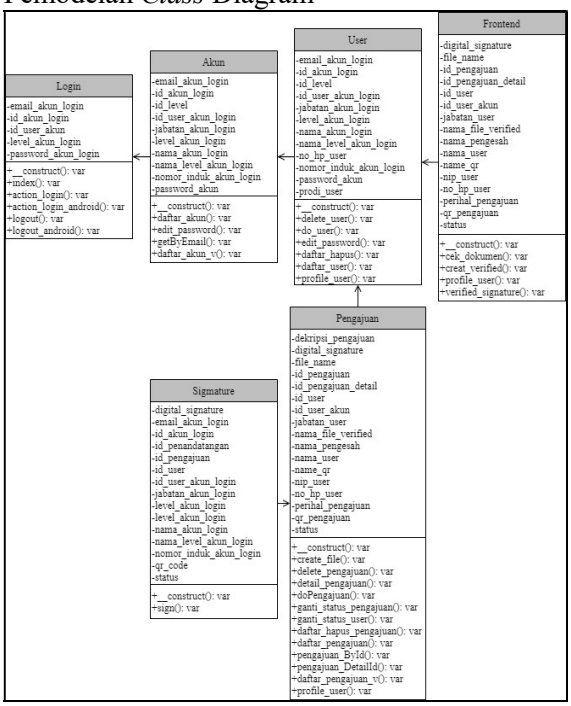


Gambar 15. *Sequence* Diagram Manajemen *User*



Gambar 16. *Sequence* Verifikasi Tandatangan

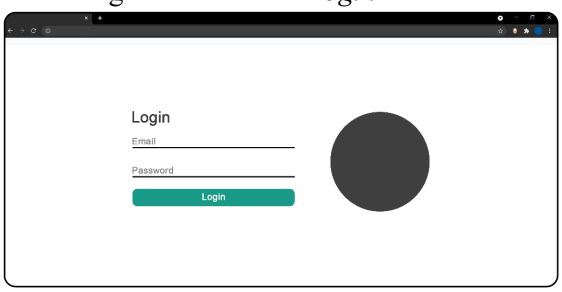
4. Pemodelan *Class* Diagram



Gambar 17. *Class* Diagram

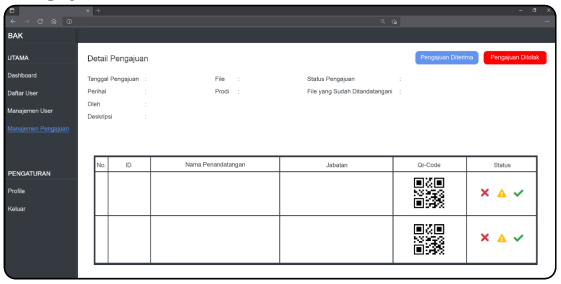
3.3. Perancangan Antar Muka

1. Perancangan Antar Muka *Login*

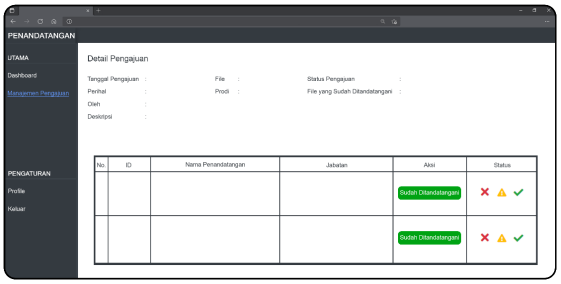


Gambar 18. Perancangan Antar Muka *Login*

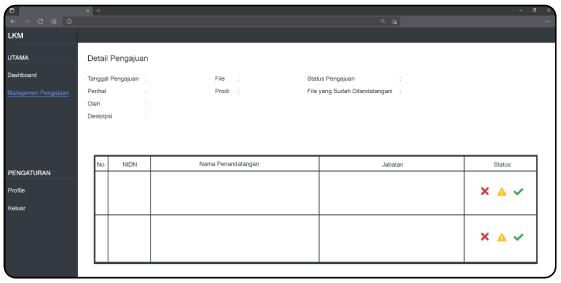
2. Perancangan Antar Muka Lihat Detail Pengajuan



Gambar 19. Perancangan Antar Muka Lihat Detail Pengajuan (Pihak Akademik)

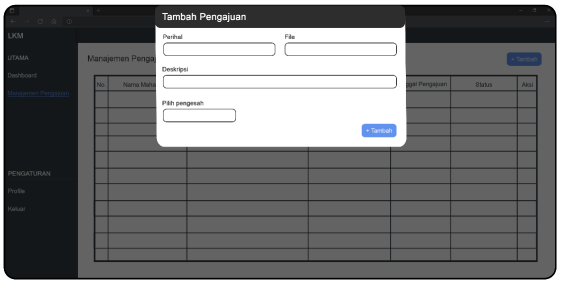


Gambar 20. Perancangan Antar Muka Lihat Detail Pengajuan (Pihak Penandatangan)



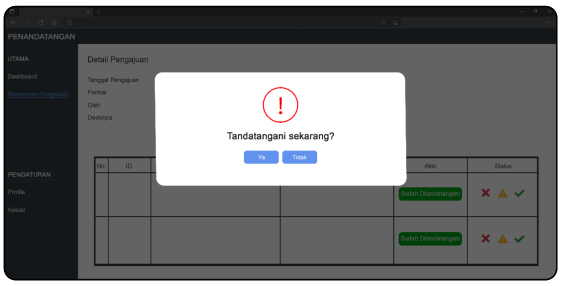
Gambar 21. Perancangan Antar Muka Lihat Detail Pengajuan (Lembaga Keluarga Mahasiswa)

3. Perancangan Antar Muka Tambah Pengajuan Dokumen



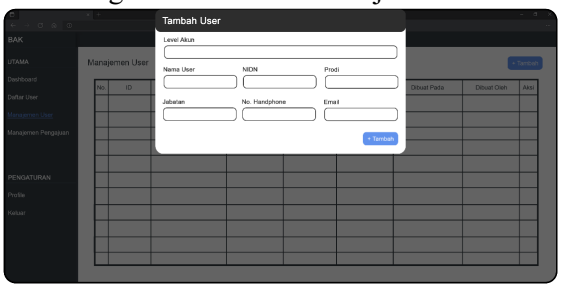
Gambar 22. Perancangan Antar Muka Tambah Pengajuan Dokumen

4. Perancangan Antar Muka Penandatanganan Dokumen



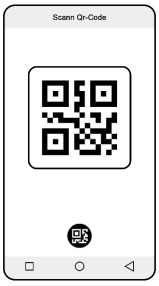
Gambar 23. Perancangan Antar Muka Penandatanganan Dokumen

5. Perancangan Antar Muka Manajemen *User*



Gambar 24. Perancangan Antar Muka Manajemen *User*

6. Perancangan Antar Muka Verifikasi Tandatangan



Gambar 25. Perancangan Antar Muka Verifikasi Tandatangan

3.4. Implementasi Algoritma

1. *Source Code Secure Hash Algorithm*-256

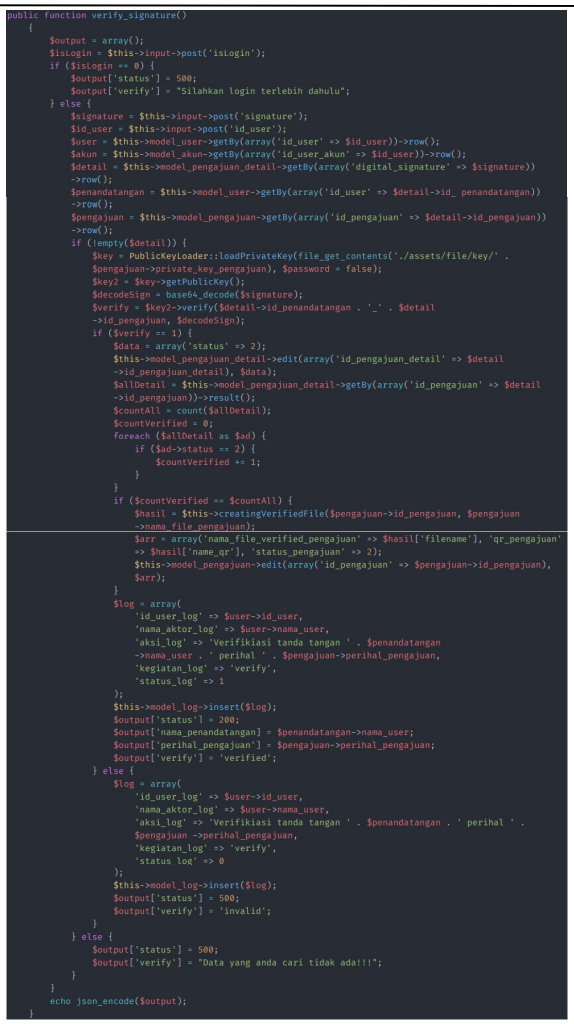
```
if ($hash == 'sha512/224' || $hash == 'sha512/256') {
        if (version_compare(PHP_VERSION, '7.1.0') < 0) {
            $initial = $hash == 'sha512/256' ?
                [
                    '22312194FC2BF72C', '9F555FA3C84C64C2', '2393B86B6F53B151', '963877195940EABD',
                    '96283EE2A88EFFE3', 'BE5E1E2553863992', '2B0199FC2C85B8AA', '0EB72DDC81C52CA2'
                ] :
                [
                    '8C3D37C819544DA2', '73E1996689DCD4D6', '1DFAB7AE32FF9C82', '679DD514582F9FCF',
                    '0F6D2B697BD44DA8', '77E36F7304C48942', '3F9D85A86A1D36C8', '1112E6AD91D692A1'
                ];
            for ($i = 0; $i < 8; $i++) {
                $initial[$i] = new BigInteger($initial[$i], 16);
                $initial[$i]->setPrecision(64);
            }

            $this->parameters = compact('initial');

            $hash = ['phpseclib3\Crypt\Hash', 'sha256'];
        }
    }
```

Gambar 26. *Source Code Secure Hash Algorithm*-256

Gambar 27. *Source Code* Pemanggilan *Secure Hash Algorithm*-256

2. *Source Code Rivest Shamir Adleman*

Gambar 28. *Source Code Rivest Shamir Adleman*



Gambar 29. *Source Code* Pemanggilan *Rivest Shamir Adleman*

Gambar 30. *Private Key*

3. *Source code Quick Response Code (QR-Code)*

```
class Ciqrcode
{
    var $cacheable = true;
    var $cachedir = 'application/cache/';
    var $errorlog = 'application/logs/';
    var $quality = true;
    var $size = 1024;

    function __construct($config = array())
    {
        include "qrcode/qrconst.php";
        include "qrcode/qrtools.php";
        include "qrcode/qrspec.php";
        include "qrcode/qrimage.php";
        include "qrcode/qrinput.php";
        include "qrcode/qrbitstream.php";
        include "qrcode/qrsplit.php";
        include "qrcode/qrrscode.php";
        include "qrcode/qrmask.php";
        include "qrcode/qrencode.php";
        $this->initialize($config);
    }
    public function initialize($config = array())
    {
        $this->cacheable = (isset($config['cacheable'])) ? $config['cacheable'] : $this->cacheable;
        $this->cachedir = (isset($config['cachedir'])) ? $config['cachedir'] : FCPATH . $this->cachedir;
        $this->errorlog = (isset($config['errorlog'])) ? $config['errorlog'] : FCPATH . $this->errorlog;
        $this->quality = (isset($config['quality'])) ? $config['quality'] : $this->quality;
        $this->size = (isset($config['size'])) ? $config['size'] : $this->size;
        if (!defined('QR_CACHEABLE')) define('QR_CACHEABLE', $this->cacheable);
        if (!defined('QR_CACHE_DIR')) define('QR_CACHE_DIR', $this->cachedir);
        if (!defined('QR_LOG_DIR')) define('QR_LOG_DIR', $this->errorlog);
        if ($this->quality) {
            if (!defined('QR_FIND_BEST_MASK')) define('QR_FIND_BEST_MASK', true);
        } else {
            if (!defined('QR_FIND_BEST_MASK')) define('QR_FIND_BEST_MASK', false);
            if (!defined('QR_DEFAULT_MASK')) define('QR_DEFAULT_MASK', $this->quality);
        }
        if (!defined('QR_FIND_FROM_RANDOM')) define('QR_FIND_FROM_RANDOM', false);
        if (!defined('QR_PNG_MAXIMUM_SIZE')) define('QR_PNG_MAXIMUM_SIZE',  $this->size);
    }
    public function generate($params = array())
    {
        if (
            isset($params['black'])
            && is_array($params['black'])
            && count($params['black']) == 3
            && array_filter($params['black'], 'is_int') === $params['black']
        ) {
            QRimage::$black = $params['black'];
        }
        if (
            isset($params['white'])
            && is_array($params['white'])
            && count($params['white']) == 3
            && array_filter($params['white'], 'is_int') === $params['white']
        ) {
            QRimage::$white = $params['white'];
        }
        $params['data'] = (isset($params['data'])) ? $params['data'] : 'QR Code Library';
        if (isset($params['savename'])) {
            $level = 'L';
            if (isset($params['level']) && in_array($params['level'], array('L', 'M', 'Q', 'H')))
            $level = $params['level'];
            $size = 4;
            if (isset($params['size'])) $size = min(max((int)$params['size'], 1), 10);
            QRcode::png($params['data'], $params['savename'], $level, $size, 2);
            return $params['savename'];
        } else {
            $level = 'L';
            if (isset($params['level']) && in_array($params['level'], array('L', 'M', 'Q', 'H')))
            $level = $params['level'];
            $size = 4;
            if (isset($params['size'])) $size = min(max((int)$params['size'], 1), 10);
            QRcode::png($params['data'], NULL, $level, $size, 2);
        }
    }
}
```

Gambar 31. *Source Code Quick Response Code (QR-Code)*

```
public function sign()
    {
        $id_pengajuan = $this->input->post('id');
        $pengajuan = $this->model_pengajuan->getBy(array('id_pengajuan' => $id_pengajuan))->row();
        $detail = $this->model_pengajuan_detail->getBy(array('id_pengajuan' => $id_pengajuan,
        'id_penandatangan => $this->id_user))->row();
        $key = PublicKeyLoader::loadPrivateKey(file_get_contents('./assets/file/key/' . $pengajuan
        ->private_key_pengajuan), $password = false);
        $sign = base64_encode($key->sign($this->id_user . '_' . $id_pengajuan));
        $this->load->library('ciqrcode');
        $config['cacheable']    = true;
        $config['cachedir']     = './assets/';
        $config['errorlog']     = './assets/';
        $config['imagedir']     = './assets/file/images/';
        $config['quality']      = true;
        $config['size']         = '1024';
        $config['black']        = array(224, 255, 255);
        $config['white']        = array(70, 130, 180);
        $this->ciqrcode->initialize($config);
        $image_name = sha256($this->id_user) . '.png';
        $params['data'] = $sign;
        $params['level'] = 'M';
        $params['size'] = 10;
        $params['savename'] = FCPATH . $config['imagedir'] . $image_name;
        $this->ciqrcode->generate($params);
        $data = array('digital_signature' => $sign, 'qr_code' => $image_name, 'status' => 1);
        $process = $this->model_pengajuan_detail->edit(array('id_pengajuan' => $id_pengajuan,
        'id_penandatangan =>$this->id_user), $data);
        $log = array(
            'nama_aktor_log' => $this->content['nama_akun_login'],
            'aksi_log' => 'User ' . $this->content['nama_akun_login'] .
            ' Melakukan Tanda Tangan Pada Pengajuan ' . $pengajuan->perihal_pengajuan,
        );
        $this->model_log->insert($log);
        $output = array();
        if ($process) {
            $output['cond'] = '1';
            $output['msg'] = "Berhasil Menandatangani!!!";
        } else {
            $output['cond'] = '0';
            $output['msg'] = "Gagal Menandatangani!!!";
        }
        echo json_encode($output);
    }
```

Gambar 32. *Source Code* Pemanggilan *Quick Response Code (QR-Code)*

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah diuraikan pada bab sebelumnya, dapat disimpulkan beberapa hal mengenai simpulan yaitu :

1. Aplikasi dapat mempermudah pihak pemohon tanda tangan yaitu Lembaga Keluarga Mahasiswa (LKM).
2. Aplikasi dapat mempermudah Penandatangan dengan memberikan tanda tangan digital.
3. Aplikasi dapat mengamankan tanda tangan digital agar tidak terjadi pemalsuan menggunakan *Secure Hash Algorithm (SHA)*-256 dan *Rivest Shamir Adleman (RSA)*.
4. Aplikasi dapat memvalidasi keabsahan tanda tangan dengan bantuan *Quick Response Code (QR-Code)*.

DAFTAR PUSTAKA

[1] T. Ariani, Pembelajaran Kooperatif Tipe Team Assisted Individualization (TAI): Dampak Terhadap Hasil Belajar Fisika Siswa, Jurnal Ilmiah Pendidikan Fisika Al-Biruni. 6 (2017) 169–177. https://doi.org/10.24042/jipfalbiruni.v6i2.1802.

[2] E.J. Istiyanto, P.A. Widodo, Karakteristik Metodologi Penelitian Bidang Ilmu Komputer (Ik) Berlandaskan Pendekatai\ Positivistik, Jurnal Sains Dan Matematika. 17 (2009) 115–120.

[3] Sommerville, I. (2011). Software engineering 9th Edition. ISBN-10, 137035152, 18.