RANCANG BANGUN APLIKASI PENGAMANAN KEASLIAN SURAT IZIN TEMPAT USAHA MENGGUNAKAN ALGORITMA *ELGAMAL* DAN *SECURE HASH ALGORITHM 256* STUDI KASUS: BADAN PELAYANAN PERIZINAN TERPADU (BPPT) KOTA BENGKULU

Sandi Yusmantoro[1], Edy Hermansyah[2], Rusdi Efendi[3]

[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Bengkulu
Jl. W.R. Supratman Kandang Limun Bengkulu 38371 A
Telp. (0736) 344087, 21170 – 227

[1]ndhy.detektif@gmail.com

Abstrak: Surat Izin Tempat Usaha (SITU) berisi informasi mengenai data perusahaan, pemilik perusahaan dan identitas SITU. Walaupun informasi pada SITU bersifat unik, tetapi masih ada saja pihak yang dengan sengaja memalsukan SITU. Oleh karena itu penulis bermaksud untuk membangun aplikasi pengamanan keaslian SITU menggunakan algoritma ElGamal dan Secure Hash Algorihtm 256 (SHA-256). Algoritma ElGamal digunakan untuk mengenkripsi informasi yang terdapat pada SITU. Sedangkan SHA-256 digunakan untuk mengubah dan memperpendek *ciphertext* yang dihasilkan oleh algoritma ElGamal menjadi *message digest* yang panjangnya 256 bit. Hal tersebut dilakukan agar lebih efisien dalam menyisipkan kode pengamanan pada setiap SITU. Proses autentikasi SITU dapat dilakukan dengan menggunakan kode pengamanan tersebut. Sebagai alternatif untuk melakukan autentikasi SITU, penulis menambahkan *Data Matrix* yang berisi kode pengamanan pada setiap SITU, kemudian untuk dapat membaca *Data Matrix* tersebut penulis menggunakan smart phone berbasis Android. Aplikasi ini dibangun menggunakan bahasa pemrograman Java. Dan metode pengembangan sistem pada aplikasi ini menggunakan metode *Waterfall.* Sedangkan metode untuk perancangan sistem, penulis menggunakan *Unified Modeling Language* (UML). Hasil akhir dari penelitian ini adalah terciptanya suatu aplikasi pengamanan keaslian SITU yang dapat digunakan mengamankan keaslian SITU dan melakukan autentikasi SITU.

Kata kunci: Pengamanan keaslian SITU, ElGamal, *SHA-256,* Kode Pengamanan, Autentikasi.

Abstract: **Place of business's license (SITU) contains information about the company's data, the company's owner, and the SITU's identities. Although the informations on SITU are unique,**

but there are still those who deliberately falsified the SITU. Therefore, the author intends to establish an application for SITU authenticity security using ElGamal algorithm and Secure Hash Algorithm 256 (SHA-256). ElGamal algorithm is used to encrypt the information in SITU. While SHA-256 is used to modify and shorten the ciphertext produced by ElGamal algorithm into a "message digest" 256 bits in length. This is done in order to insert the security code on each SITU more efficiently. Authentication process can be done by using the security code. As an alternative to authenticate SITU, the author add Data Matrix which contains security code on each SITU. The author use smart phone based on Android in order to read the Data Matrix. This application is built using Java programming language. System development methods in this application is using the Waterfall Method and for system design, the author use the Unified Modeling Language (UML). The final result of this research is an application for security of SITU authenticity that can be used to secure and authenticate SITU.

Key Word: Security of SITU authenticity, ElGamal, SHA-256, security code, Authentication.

I. PENDAHULUAN

Pembentukan Badan Pelayanan Perizinan Terpadu (BPPT) di Kota Bengkulu dimaksudkan untuk memberikan kemudahan pelayanan dibidang perizinan dengan prinsip dapat dipercaya, mudah, murah, cepat, dan transparan melalui satu atap (sumber: http://bppt.bengkulukota.go.id). Salah satu contoh pelayanannya adalah pelayanan pembuatan Surat Izin Tempat Usaha (SITU) di Kota Bengkulu. SITU adalah surat untuk memperoleh izin sebuah usaha di suatu lokasi dengan maksud agar tidak menimbulkan gangguan atau kerugian kepada pihak-pihak tertentu (sumber: http:// carapedia.com). Berdasarkan penjelasan diatas dapat disimpulkan bahwa SITU sangat penting untuk dimiliki oleh suatu perusahaan di Kota Bengkulu, agar perusahaan tersebut dapat dilindungi dan dibina oleh pemerintah Kota Bengkulu.

Pemegang SITU harus menyam-paikan laporan secara tertulis kepada Walikota Bengkulu melalui BPPT Kota Bengkulu, minimal dua kali dalam satu tahun dan SITU selalu diautentikasi setidaknya satu kali dalam setahun bersamaan dengan autentikasi surat izin usaha lainnya. SITU memiliki informasi mengenai data perusahaan, pemilik perusahaan dan identitas SITU yang berupa nomor SITU, nama pemilik peru-sahaan, pekerjaan pemilik perusahaan, nama perusahaan, alamat perusahaan, untuk siapakah SITU tersebut, prakua-lifikasi suatu perusahaan, golongan suatu perusahaan, tanggal penetapan SITU, daerah penetapan SITU, nama pengesah SITU dan tanda tangan pengesah SITU. Walaupun informasi pada SITU bersifat unik, tetapi masih ada saja pihak yang dengan sengaja memalsukan SITU untuk maksud-maksud tertentu. Salah satu kasus yang pernah terjadi adalah ketika daerah domisili perusahaan berpindah tempat, perusahaan tersebut dengan sengaja mengubah nama daerah penetapan SITU tanpa melaporkannya secara tertulis kepada Walikota Bengkulu melalui BPPT Kota Bengkulu. Hal itu tentu saja merugikan daerah dari domisili perusa-haan yang bersangkutan. Oleh karena itu untuk mengamankan keaslian SITU, diperlukan suatu metode penyandian yang disebut dengan kriptografi.

Algoritma kriptografi kunci-nirsimetri yang digunakan penulis dalam penelitian ini yaitu algoritma ElGamal. Selain algoritma ElGamal penulis juga menggunakan salah satu fungsi *hash* satu-arah, yaitu *Secure Hash Algorithm* 256.

Dalam hal ini, penulis meng-gunakan algoritma ElGamal untuk mengenkripsi data perusahaan, pemilik perusahaan dan identitas SITU, kecuali tanda tangan pengesah SITU. Dikarenakan c*iphertext* yang dihasilkan oleh algoritma ElGamal memiliki panjang dua kali lipat dari panjang pesan yang dienkripsi, misalnya panjang pesan semula 300 karakter, maka akan meng-hasilkan *ciphertext* yang panjangnya 600 karakter. Tentunya, 600 karakter ini tidak efisien jika kita sisipkan pada SITU. Oleh karena itu penulis menggunakan SHA-256 untuk mengubah dan memperpendek *ciphertext* yang dihasil-kan oleh algoritma ElGamal menjadi *message digest* yang panjangnya 256 bit atau 64 karakter dalam heksadesimal. Hal tersebut dilakukan agar lebih efisien dalam menyisipkan karakter (kode pengamanan) pada setiap SITU yang dicetak. Jadi dengan kode pengamanan itulah, kita dapat mendekripsikan pesan, kemudian melakukan autentikasi SITU.

Sebagai alternatif untuk mendek-ripsikan pesan dan melakukan auten-tikasi SITU, penulis menambahkan *Data Matrix* yang berisi kode pengamanan SITU pada setiap SITU yang dicetak. Untuk dapat membaca *Data Matrix* tersebut, penulis menggunakan *smartphone* berbasis android. Setelah dibaca, barulah pesan tersebut dapat didekripsikan dan diautentikasi menggunakan *smartphone* tersebut.

Berdasarkan penjelasan diatas, maka penulis bermaksud untuk mengamankan keaslian SITU dengan mengangkat judul "Rancang Bangun Aplikasi Pengamanan Keaslian Surat Izin Tempat Usaha Menggunakan Algoritma ElGamal dan *Secure Hash Algorithm* 256".

II. LANDASAN TEORI

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [5].

Menurut Menezes dan Vanstone (dalam Munir, 2006:9) terdapat empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, yaitu:

1. Kerahasiaan
2. Integritas data
3. Autentikasi
4. Nirpenyangkalan

A. Algoritma Kriptografi

Ada dua macam algoritma kunci di dalam kriptografi, yaitu algoritma kunci-simetri dan algoritma kunci-nirsimetri. Algoritma kunci simetri mengharuskan pengirim dan penerima pesan menyetujui suatu kunci tertentu sebelum mereka berkomunikasi. Contohnya RC6, Twofish, Rijndael (AES), Blowfish, DES dan lainnya. Sedangkan algoritma kunci-nirsimetri, menggunakan dua jenis kunci, yaitu kunci publik yang digunakan untuk mengenkripsi pesan dan kunci rahasia yang digunakan untuk mendekripsi pesan. Contoh dari algoritma kunci-nirsimetri adalah RSA, ElGamal, McEliece, LUC, dan DSA (*Digital Signature Algorithm*).

B. Algoritma ElGamal

Algoritma ElGamal dibuat oleh Taher ElGamal pada tahun 1984. Algoritma ini pada mulanya digunakan untuk tanda tangan digital, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan dekripsi. Besaran-

besaran yang digunakan didalam algoritma ElGamal adalah sebagai berikut [5]:

a. Bilangan prima, *p* (tidak rahasia)
b. Bilangan acak, *g (g<p)* (tidak rahasia)
c. Bilangan acak, *x (x<p)* (rahasia, kunci privat)
d. $y = g^x \bmod p$ (tidak rahasia, kunci publik)
e. *m* (plainteks) (rahasia)
f. a dan b (cipherteks) (tidak rahasia)

1) Algoritma Membangkitkan Pasangan Kunci

Sebelum memulai proses enkripsi dan dekripsi, kita perlu membangkitkan pasangan kunci terlebih dahulu, berikut algoritma untuk membangkitkan pasangan kunci [5]:

a. Pilih sembarang bilangan prima *p* (*p* dapat dibagikan diantara anggota kelompok).
b. Pilih dua buah bilangan acak, *g* dan *x*, dengan syarat $g < p$ dan $1 \leq x \leq p-2$
c. Hitung $y = g^x \bmod p$.

Hasil dari algoritma ini:

Kunci publik : tripel (y,g,p)

Kunci privat : pasangan (x, p)

Dari keterangan diatas dapat diketahui bahwa nilai *g* dan *p* tidak rahasia, sebab nilai tersebut diperlukan pada perhitungan enkripsi dan dekripsi.

2) Algoritma Enkripsi/Dekripsi

Berikut proses enkripsi dan dekripsi algoritma ElGamal [5]:

a) *Enkripsi:*
   1. Susun plainteks menjadi blok-blok m1, m2,…, sedemikian sehingga setiap blok mempresentasikan nilai di dalam selang [0,p-1].
   2. Pilih bilangan acak *k*, yang dalam hal ini $1 \leq k \leq p-2$.
   3. Setiap blok m dienkripsi dengan rumus:

      $a = g^k \bmod p$ . . . (2.1)

      $b = y^k m \bmod p$ . . . (2.2)

b) Dekripsi:
   1. Gunakan kunci privat *x* untuk mendekripsi a dan b menjadi plainteks *m* dengan persamaan:

      $m = b/a^x \bmod p$ . . . (2.3)

      catatan $(a^x)^{-1} = a^{p-1-x} \bmod p$.

C. Secure Hash Algorithm 256 (SHA-256)

SHA-256 dirancang oleh *The National Institute of Standards and Technology* (NIST) pada tahun 2002. SHA-256 menghasilkan *message digest* dengan panjang 256 bit. SHA-256 merupakan salah satu fungsi *hash* satu arah, karena tidak mungkin menemukan pesan dari *message digest* yang dihasilkan.

SHA-256 menggunakan enam fungsi logika, di mana setiap fungsi beroperasi pada 32-bit, yang direpresentasikan sebagai x, y, dan z [6]. Berikut enam fungsi logika tersebut:

$$Ch(x,y,z) = (x \wedge y) \oplus (x \wedge z)$$

$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \quad \ldots (2.5)$$

$$\sum_0 (x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \quad \ldots (2.6)$$

$$\sum_1 (x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x) \quad \ldots (2.7)$$

$$\sigma_0 = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x) \ldots (2.8)$$

$$\sigma_1 = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x) \ldots (2.9)$$

Selain enam fungsi logika yang digunakan, SHA-256 juga meng-gunakan nilai konstanta K [0..63]. Berikut nilai konstanta K[0..63] [6]:

Tabel 1. Nilai K[0..63]

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

Proses untuk menghasilkan *message digest* pada SHA-256 ini meliputi lima tahapan [6], berikut kelima tahapan tersebut:

1. Penambahan Bit-Bit Pengganjal (*Message padding)*
2. Penambahan Nilai Panjang Pesan Semula
3. Inisialisasi Nilai H*ash* Awal
4. Pengolahan Pesan Dalam Blok Berukuran 512 Bit
5. *Output*

Hasil akhir dari semua proses tersebut akan didapatkan 256 bit *message digest* untuk pesan M, yaitu:

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$$

D. Barcode

Kode batang (*barcode)* yang berbentuk garis yang mengandung kumpulan kombinasi lebar garis dan spasi garis paralel dapat disebut sebagai *barcode* satu dimensi. Sedangkan *barcode* yang berbentuk persegi, titik, heksagon, dan bentuk geometri lainnya dapat disebut *barcode* dua dimensi [7]:

Data Matrix merupakan salah satu contoh *barcode* dua dimensi. *Data Ma-trix* ini mampu menyimpan 2.335 karak-ter *alphanumeric* [8].

E. Android

Android dikembangkan oleh Google bersama *Open Handset Allience* (OHA) yaitu aliansi perangkat selular terbuka yang terdiri dari 34 perusahaan *Hardware*, *Software*, dan perusahaan telekomunikasi ditujukan untuk mengembangkan standar terbuka bagi perangkat selular.

F. Metode Pengembangan Sistem

Metode Pengembangan sistem yang digunakan oleh penulis adalah *waterfall*. Tahapan-tahapan dalam pengembangan sistem ini adalah sebagai berikut:

1. Penelitian Awal
2. Definisi Kebutuhan
3. Perancangan Sistem
4. Pengkodean dan Pengujian

   Pengkodean perangkat lunak menggunakan bahasa pemrograman Java dengan *editor* NetBeans IDE 7.0 dan Eclipse Galileo dan pengkodean *database* menggunakan MySQL dengan editor MySQL GUI Tools 5.0.
5. Pengujian menggunakan *Black Box testing*, yang meliputi:
   a. validasi,
   b. Desain tes,
   c. *Interface*,
   d. *Database*,
   e. Analisa kinerja sistem.
6. Implementasi
7. Pengoperasian dan Dukungan

III. METODOLOGI

A. Analisis Sistem

Di dalam analisis sistem terdapat langkah-langkah dasar yang harus dilakukan oleh Analis Sistem yaitu *Identify*, *Understand*, *Analyze*, *Report* [9].

B. Business Process (Proses Bisnis)

Tabel 2 Business Process

No	Aktivitas	Pihak yang terlibat
1	Pembuatan SITU	1.Pemohon SITU (1.1) (1.2) (1.6) 2.Karyawan BPPT Kota

		Bengkulu (1.3) (1.4) 3.Kepala BPPT Kota Bengkulu (1.5)
2	Penyimpanan data SITU	1.Karyawan BPPT Kota Bengkulu (2.1)
3	Autentikasi SITU	1.Pemilik SITU (3.1) 2.Karyawan BPPT Kota Bengkulu (3.2) (3.2.1)

Rule:

1.1 Mengajukan surat permohonan SITU.
1.2 Melengkapi persyaratan pembuatan SITU.
1.3 Memeriksa tempat usaha pemohon SITU
1.4 Membuat SITU.
1.5 Menandatangani SITU.
1.6 Mengambil SITU.
2.1 Menyimpan data SITU yang dibuat menggunakan Microsoft Office Word dan Excel pada sebuah komputer.
3.1 Memberikan izin kepada karyawan BPPT Kota Bengkulu untuk melakukan autentikasi SITU.
3.2 Melakukan Autentikasi SITU.
3.2.1 Memeriksa apakah data SITU masih sama dengan data yang dimiliki BPPT Kota Bengkulu.

C. Perancangan Sistem

Untuk perancangan sistem penulis menggunakan pemrograman berorientasi objek. Konsep-konsep berorientasi objek tersebut akan dijelaskan sebagai berikut:

1. Pembungkusan
2. Pewarisan
3. Polimorfisme

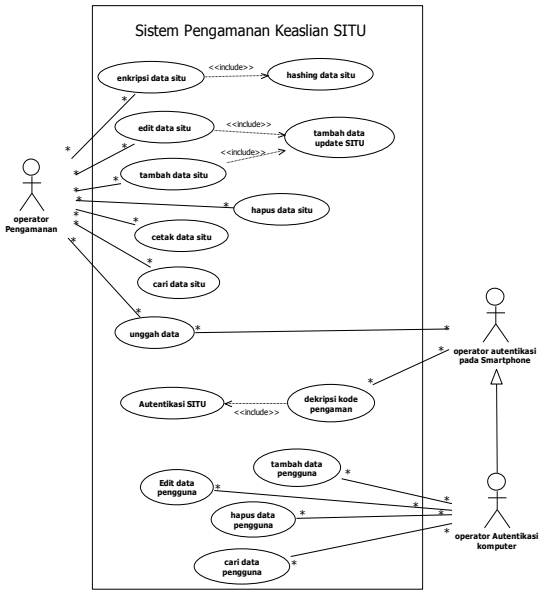
Dari penjelasan diatas dapat disimpulkan bahwa pemrograman berorientasi objek membuat pemrograman menjadi lebih mudah dan cepat, karena setiap persoalan program dilihat sebagai objek yang memiliki sekumpulan data dan metode yang dapat digabungkan.

1) Unified Modelling Language (UML)

UML adalah sebuah bahasa yang telah menjadi standar dalam industri untuk visualisasi, merancang, dan mendokumentasikan sistem perangkat lunak [3].

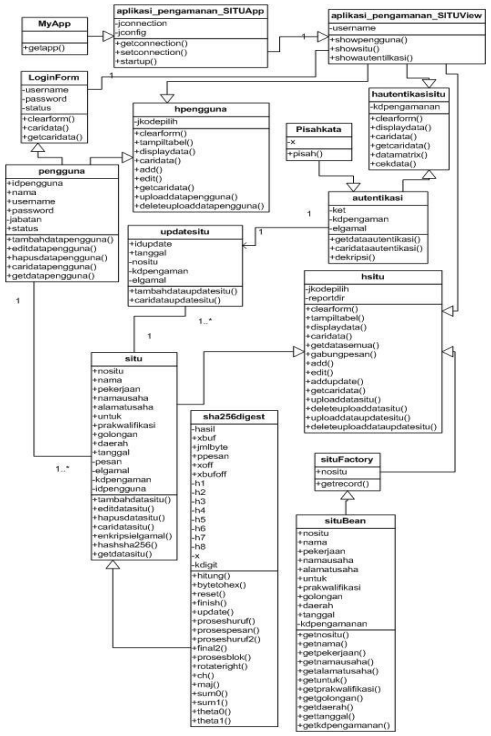
Penulis menggunakan UML versi 2.0 tersebut terdiri dari empat belas teknik diagram UML yang dapat digunakan untuk memodelkan suatu sistem. Empat belas teknik diagram tersebut dapat dibagi menjadi dua kelompok utama [2]: satu untuk pemodelan struktur suatu sistem dan satu lagi untuk pemodelan sifat suatu sistem. S*tructure diagrams* terdiri dari *class diagram, object diagram, package diagram, deployment diagram, component diagram,* dan *composite structure diagram.* Sedangkan *behavior diagrams* terdiri dari *activity diagram, sequence diagram, communication diagram, interaction overview diagram, timing diagram, behavior state machine diagram, protocol state machine diagram,* dan *use case diagram*.

a. Use Case Diagram



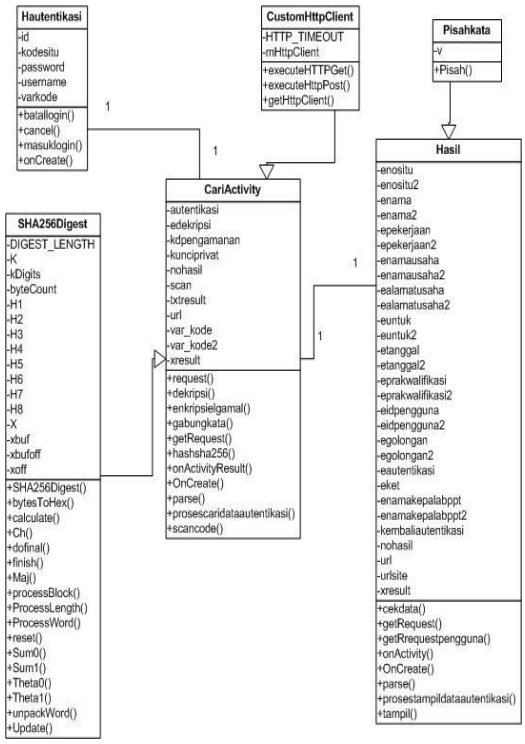
Gambar 1. *Use Case Diagram*

b. Class Diagram



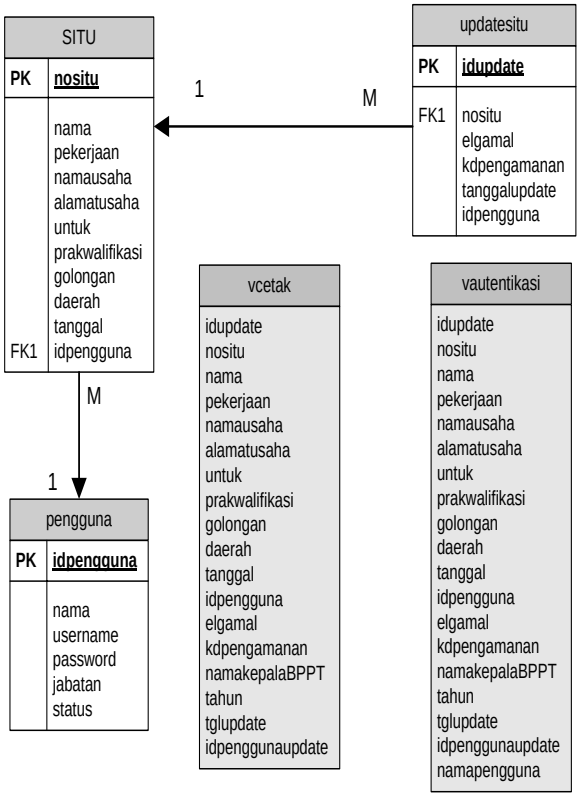
Gambar 2. *Class Diagram* Aplikasi Pengamanan Keaslian SITU

Class Diagram Pada Smartphone



Gambar 3. *Class Diagram* Aplikasi Pengamanan Keaslian SITU pada *Smartphone*

2) Perancangan Table Relationship



Gambar 4. *Table Relationship* Aplikasi Pengamanan Keaslian SITU

3) Perancangan User Interface

Tujuan utama perancangan *user interface* adalah untuk mempermudah pengguna dalam mengoperasikan sistem. Berikut rancangan *user interface* aplikasi pengamanan keaslian SITU.

IV. HASIL DAN PEMBAHASAN

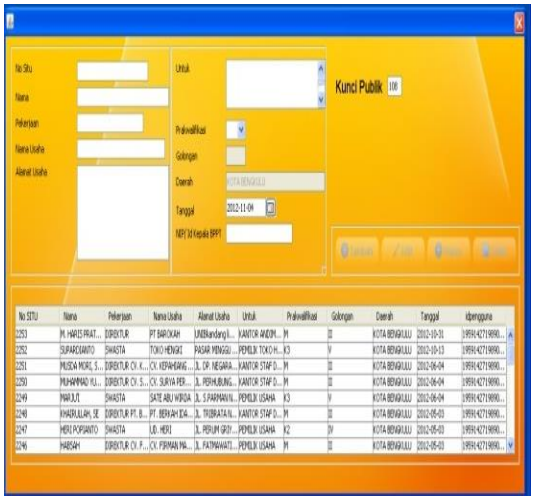
A. Tampilan Halaman Menu Utama

Pada halaman ini menu sebelah kanan akan aktif sesuai hak akses pengguna yang melakukan login.

Gambar 5. Tampilan Halaman Menu Utama

B. Tampilan Halaman Pengamanan SITU

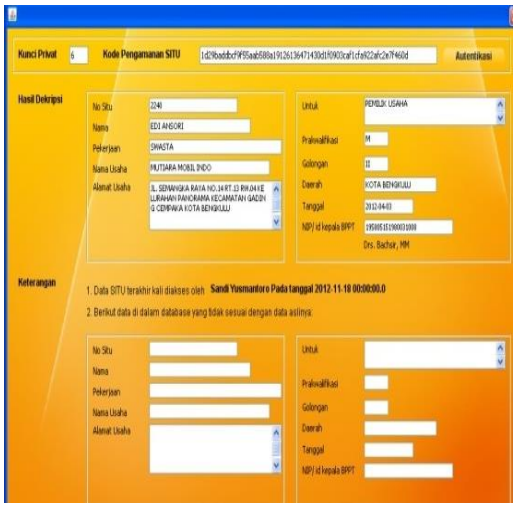
Halaman ini digunakan untuk mencetak SITU yang telah diberikan kode pengamanan.



Gambar 6. Tampilan Halaman Pengamanan SITU

C. Halaman Autentikasi SITU

Halaman ini digunakan untuk mengautentikasi SITU dengan cara mendekripsikan kode pengamanan yang telah disisipi pada SITU, sehingga kita dapat mengetahui apakah data SITU tersebut telah diubah atau tidak.



Gambar 7. Tampilan Halaman

D. Halaman Hasil Autentikasi SITU pada Smartphone

Halaman ini merupakan hala-man yang memuat hasil dekripsi kode pengamanan yang dilakukan menggunakan smartphone.

Gambar 8. Tampilan Halaman Hasil Autentikasi SITU pada *Smartphone*

V. KESIMPULAN

Berdasarkan analisis, hasil dan pembahasan, maka terdapat beberapa hal yang dapat disimpulkan, yaitu:

1. Menghasilkan sebuah aplikasi pengamanan keaslian SITU yang dapat digunakan untuk

mengamankan keaslian SITU dan melakukan autentikasi SITU.

2. Dengan adanya aplikasi ini, dapat mengetahui operator yang terakhir kali melakukan perubahan data pada setiap SITU.
3. Aplikasi pengamanan keaslian SITU ini dapat diimplementasikan pada perangkat komputer dan *smartphone* berbasis android minimal versi 2.2 froyo dan aplikasi ini dapat berjalan dengan baik tanpa ada *error*.
4. Aplikasi pengamanan keaslian SITU ini juga telah dipresentasikan kepada karyawan BPPT Kota Bengkulu, dengan hasil layak untuk digunakan dalam meminimalisir pemalsuan SITU di Kota Bengkulu

VI. SARAN

Saran yang dapat disampaikan oleh penulis adalah:

1. BPPT Kota Bengkulu merupakan instansi pemerintah dan penggunaan aplikasi pada instansi pemerintah harus mendapat izin dari pemerintah pusat. Penulis belum diizinkan untuk mengakses server pusat dengan alasan keamanan. Penulis berharap aplikasi dapat mengakses server pusat agar aplikasi dapat digunakan diseluruh Indonesia khususnya di Kota Bengkulu.
2. Untuk mempermudah memasukkan kode pengamanan SITU pada aplikasi pengamanan keaslian SITU di komputer, sebaiknya menggunakan mesin *barcode reader*.

REFERENSI

[1] Bengkulukota. 2011. Surat Izin Tempat Usaha. [Online]. Tersedia: http://bppt.bengkulukota.go.id/index.php/perizinan/jenis-perizinan/11-surat-izin-tempat-usaha-situ.html. [30 April 2012].

[2] Dennis *et al*. 2005. *System Analysis and Design with uml version 2.0*. United States of Americ: A Wiley-Interscience Publication.

[3] Huda, Miftakhul dan Bunafit Nugroho. 2010. *Membuat Aplikasi Database dengan Java, MySQL, dan NetBeans*. Jakarta: PT. Elex Media Komputindo.

[4] Mini. 2012. Contoh Surat Izin Tempat Usaha. [Online]. Tersedia: http://carapedia.com/surat_ijin_tempat_usaha_info266.html. [03 Maret 2012].

[5] Munir, Rinaldi. 2006. *Kriptografi*.Bandung : Informatika.

[6] NIST. 2002 .Announcing the Secure Hash Standard. [Online]. Tersedia: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf [1 September 2012]

[7] Yudhanto, Yudha. 2011. Sejarah Teknologi Barcode. [Online]. Tersedia: http://ilmukomputer.org/wp-content/uploads/2011/03/sejarah-barcode-yudha.pdf [20 September 2012]

[8] Wahyono, Teguh. 2010. *Membuat Sendiri Aplikasi Dengan Memanfaatkan Barcode*. Jakarta: PT. Elex Media Komputindo.

[9] _____. 2012. Analisis Sistem. *Mercubuana.* [Online]. Tersedia: http://journal.mercubuana.ac.id/data/Analisis%20Sistem.doc [17 Juli 2012]