SISTEM KOMUNIKASI FULL DUPLEX UNTUK KEAMANAN UJIAN *ONLINE* CLIENT-SERVER DENGAN METODE ENKRIPSI ALGORITMA *BLOWFISH* MENGGUNAKAN PLATFORM ANDROID DAN WEB

[1]Jan Edward Gunster Fangohoi, [2]Eng.I komang Somawirata, [3]M.Ibrahim Ashari.
Institut Teknologi Nasional, Malang, Indonesia,
[1]edwardvhe061013@gmail.com, [2]bryan_130572@yahoo.com, [3]sotyohadi@yahoo.com

Abstrak— Ujian merupakan salah satu wujud evaluasi dari proses belajar. Sejauh mana pemahaman siswa terhadap bidang studi yang ditempuh diukur melalui hasil yang diperoleh setelah melaksanakan ujian. Perkembangan model pelaksanaan ujian pun kini menyesuaikan perkembangan teknologi dimana saat ini sudah umum diadakan ujian secara online yang menggeser pelaksanaan ujian konvensional yang mengharuskan penguji melakukan evaluasi secara manual pada lembar jawaban.

Seiring dengan banyaknya pengguna mobile device di seluruh dunia yang mencapai lebih dari 2,23 miliar [EMR-14], Penelitian ini memanfaatkan mobile device sebagai client dari sistem ujian online. Penggunaan mobile device sebagai alternatif client dari personal computer dapat meningkatkan fleksibilitas karena mobile device dapat dengan mudah dibawa kemana saja dibandingkan dengan personal computer.

Kata kunci : Ujian Online, Komunikasi full Full duplex

I. PENDAHULUAN

Ujian merupakan salah satu wujud evaluasi dari proses belajar. Sejauh mana pemahaman siswa terhadap bidang studi yang ditempuh diukur melalui hasil yang diperoleh setelah melaksanakan ujian. Perkembangan model pelaksanaan ujian pun kini menyesuaikan perkembangan teknologi dimana saat ini sudah umum diadakan ujian secara *online* yang menggeser pelaksanaan ujian konvensional yang mengharuskan penguji melakukan evaluasi secara manual pada lembar jawaban. Dua dari tiga unsur utama terkait keamanan data dan informasi menjadi perhatian dalam pelaksanaan ujian online ini adalah confidentiality dan integrity

Confidentiality (kerahasiaan), yang juga dapat diartikan sebagai privasi atau kerahasiaan merujuk pada perlindungan informasi dari penyingkapan pihak yang tidak sah.

integrity, dapat diartikan sebagai akurasi. Menunjuk pada perlindungan informasi, data, atau transmisi yang tidak sah, tidak terkendali, atau perubahan yang disengaja.

II. METODOLOGI

A. Ujian Online

Berdasarkan metode pengerjaannya, ujian dapat dibedakan atas ujian konvensional dan ujian online. Ujian konvensional adalah ujian yang pengerjaannya menggunakan kertas dan alat tulis dan mengharuskan peserta ujian mendatangi tempat tertentu untuk melaksanakan ujian. 2.2. Sistem dan Sistem Keamanan sistem keamanan melingkupi lima aspek, meliputi

1. Privacy / Confidentiality

Aspek privacy adalah sebuah tindakan yang dilakukan untuk menjaga informasi dari orang yang tidak berhak mengakses informasi tersebut.

2. Integrity

Aspek integrity atau integritas lebih menekankan bahwa suatu informasi tidak boleh diubah tanpa adanya izin dari pemilik informasi tersebut.

3. Authentication

Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli.

4. Availability

Aspek availability berhubungan dengan ketersediaan sebuah data atau informasi.

5. Access Control

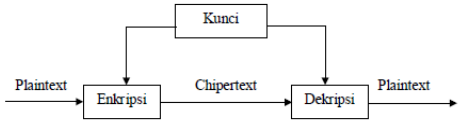
Aspek access control berhubungan dengan cara pengaturan akses kepada informasi.

B. Kriptografi

kriptografi merupakan ilmu dan seni yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data. Kriptografi sendiri mempunyai komponen untuk mencapai tujuan kriptografi.beberapa kriptografi meliputi:

1. Enkripsi (*Encryption*) : Enkripsi merupakan hal yang sangat penting dalam kriptografi untuk mengamankan sebuah informasi agar pesan yang dikirimkan terjaga kerahasiaannya.

2. Dekripsi (Decryption): Dekripsi merupakan kebalikan dari proses enkripsi. Dekripsi yaitu proses mengubah kembali pesan yang telah dienkripsi menjadi pesan aslinya, yang disebut dengan dekripsi pesan.
3. Kunc i: Kunci yang dimaksud disini adalah kunci atau sandi yang digunakan untuk melakukan enkripsi maupun dekripsi.
4. *Plaintex t: Plaintext* disebut juga *cleartext*, yaitu pesan asli yang ditulis atau diketik.
5. Pesan : Pesan bisa berupa data atau informasi yang dikirimkan (melalui kurir, saluran komunikasi data, dan sebagainy).
6. *Ciphertext : Ciphertext* merupakan pesan yang dihasilkan dari proses enkripsi. Pesan yang terkandung dalam *ciphertext* ini sulit dibaca karena berisi berbagai macam karakter tanpa arti/tidak bermakna.
7. Kriptanalisis (*Cryptanalysis*) : Dapat diartikan sebagai analisis sandi atau suatu ilmu memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Pelakunya disebut *cryptanalys* (kriptanalis).



Gambar 2.1 Skema Proses Enkripsi dan Dekripsi

C. SQL Injection

SQL Injection merupakan kegiatan menyisipkan perintah SQL dalam suatu statement SQL pada aplikasi client yang sedang berjalan. Sebagai contoh misalkan ada suatu aplikasi dengan source code seperti yang ditunjukkan Gambar

```
$SQL = "select" from login where username =
  '$username' and password = '$password'";
```

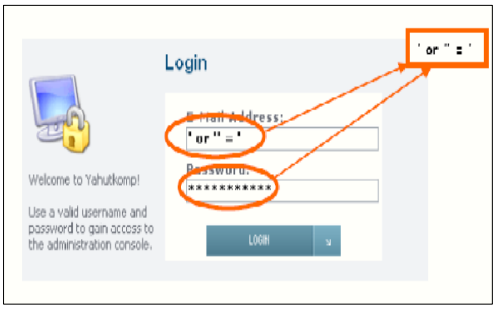
Gambar 2.2 Contoh Source Code

Memasukkan Username dan Password Dengan metode pengiriman data GET maupun POST, maka *query* pada Gambar 2.2 dapat diinjeksi dengan mengisikan string ‘or’ ‘=’ pada *login form*, sehingga hasilnya akan tampak seperti

```
$SQL = "select" from login where username =
'user' or ''='' and password = 'pass' or ''='';
```

Gambar 2.3 Contoh penggunaan *SQL Injection*

Dengan sintaks *SQL Injection* ini hasil selection akan selalu TRUE sehingga aplikasi dapat ditembus seperti dicontohkan pada Gambar 2.4



Gambar 2.4 *SQL Injection* pada form *login*

D. Aplikasi Perangkat Bergerak

Aplikasi perangkat bergerak (*mobile*) adalah suatu aplikasi yang dibuat secara khusus untuk berjalan pada *mobile device* android.

E. Java

Java adalah bahasa pemrograman tingkat tinggi yang digunakan untuk membuat dan menjalankan perangkat lunak pada komputer maupun telepon genggam [ASR-11]. Dikembangkan oleh James Gosling saat masih bergabung dengan perusahaan Sun Microsystem dan dirilis pada tahun 1995.

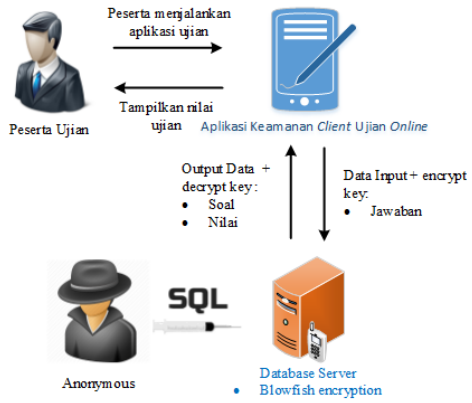
III PERANCANGAN

A. Perancangan Sistem

Perancangan arsitektur sistem yang digunakan dalam penelitian ini dilakukan setelah semua kebutuhan untuk pembuatan aplikasi yang didapatkan melalui tahap analisis kebutuhan telah terpenuhi. Perancangan sistem dibedakan menjadi dua model yaitu perancangan sistem pengiriman jawaban dan perancangan sistem perlindungan informasi jawaban.

B. Perancangan Umum Sistem Aplikasi

Perancangan umum sistem aplikasi merupakan tahap awal dari perancangan perangkat lunak. Perancangan dilakukan dengan merepresentasikan arsitektur sistem secara umum, seperti yang ditunjukkan pada Gambar :



Gambar 3 Gambaran Umum Sistem

Peserta sebagai *user* menjalankan aplikasi ujian pada *smartphone* untuk menjawaban. Selanjutnya sistem melakukan perlindungan enkripsi menggunakan metode Blowfish terhadap keamanan jawaban nilai sebagai data *input* ke dalam database ujian. Setelah pengolahan data input, sistem melakukan dekripsi terhadap *ciphertext* jawaban untuk dilakukan *scoring*. Hasil ujian berupa nilai diberi perlindungan enkripsi pula menggunakan metode Blowfish yang nantinya akan ditampilkan kembali pada peserta ujian setelah dilakukan proses dekripsi. *Anonymous* melakukan upaya masuk ke dalam database dengan tujuan dapat mengubah jawaban asal dari peserta sehingga nantinya akan berpengaruh terhadap nilai hasil ujian.

IV PENGUJIAN

A. Implementasi Algoritme dan Source Code

Pada implementasi algoritme kriptografi Blowfish dilakukan dua proses yaitu pada proses enkripsi dengan hasil nilai peserta sebagai input. Sistem akan melakukan proses enkripsi setelah peserta menjawab soal terakhir dari perangkat mobile Android. Selanjutnya akan dilakukan proses enkripsi dengan menjalankan cipher dari algoritme Blowfish pada kode baris 7. Proses enkripsi diperoleh dengan memanggil library "java.crypto.cipher" (kode baris 7-8). Hasil dari enkripsi pesan atau nilai selanjutnya diubah kembali dalam string (kode baris 9-10).

```
1. public class Nilai extends Activity implements
   OnClickListener {
2.       String Name,Pass,IP,Nilai, encryptnilai;
3.       Button btnKeluar;
4.       TextView tvNilai, tvenkripsi;
5.       public static String enkripsi(String pesan,
   String key){
6.            try {
7.                SecretKeySpec KS =
   new SecretKeySpec(key.getBytes(), "Blowfish");
8.                Cipher cipher =
   Cipher.getInstance("Blowfish");
9.                cipher.init(Cipher.ENCRYPT_MODE, KS);
10.              byte[] encrypted =
   cipher.doFinal(pesan.getBytes());
11.               return
   Base64.encodeToString(encrypted, Base64.NO_PADDING);
                  }
12.     catch (Exception e) {
                   return "ERROR:"+e.getMessage();
                   }
            }
```

```
13.     @Override
14.     protected void onCreate
   (Bundle savedInstanceState) {
15.        super.onCreate(savedInstanceState);
16.     setContentView(R.layout.nilai);
17.     Intent main=getIntent();
              // get reference to the views
18.     Name = main.getExtras().getString("Name");
19.     Pass = main.getExtras().getString("Pass");
20.     IP = main.getExtras().getString("IP");
21.     Nilai = main.getExtras().getString("Nilai");
22.     tvNilai = (TextView) findViewById(R.id.tvNilai);
23.     tvenkripsi = (TextView)
   findViewById(R.id.tvenkripsi);
24.     btnKeluar = (Button)
   findViewById(R.id.btnKeluar);
25.     encryptnilai = enkripsi(Nilai,"global34blow");

26.     if (isConnected()) {
27.     }
        // add click listener to Button "POST"
28.     tvNilai.setText(Nilai);
29.     tvenkripsi.setText(encryptnilai);
30.     btnKeluar.setOnClickListener(this);
31.     new
   HttpAsyncTask().execute("http://"+IP+"/Soalblowfish/ce
   kblowfish.php");
        }
```

Gambar 5.2 *Source code* enkripsi nilai

Dalam sistem keamanan ujian *online* telah dipasangkan kunci untuk memberi pengamanan fisik pada nilai dengan kunci "global34blow" (kode baris 25). Kunci ini pula yang nantinya digunakan untuk melakukan dekripsi pada sisi *server* setelah perangkat *mobile* terkoneksi dengan *database server* melalui alamat IP yang telah dimasukkan sebelumnya saat proses *login* melalui "cekblowfish.php" (kode baris 31)

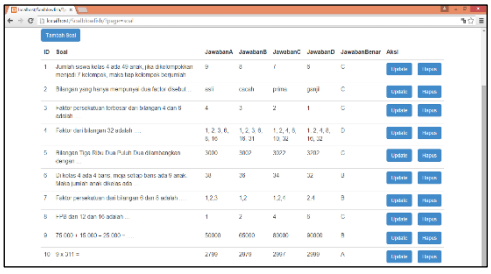
```
1. class cipher {
2.    private static $mode = 'MCRYPT_BLOWFISH';
3.    private static $key = 'global34blow';

4.    public static function decrypt ($buffer){
5.       $decoded   = base64_decode($buffer);
6.       $iv =
   mcrypt_create_iv(mcrypt_get_iv_size(constant(self::
   $mode), MCRYPT_MODE_ECB), MCRYPT_RAND);
7.       $decrypted =
   mcrypt_decrypt(constant(self::$mode), self::$key,
   $decoded, MCRYPT_MODE_ECB, $iv);
8.       if (substr($decrypted,0,1)=="0") {
9.           $decrypted=substr($decrypted,0,1);
10.      }
11.        else {
12.        if (substr($decrypted,0,3)=="100") {
13.              $decrypted=substr($decrypted,0,3); `
14.            } else {
15.              $decrypted=substr($decrypted,0,2);
16.            }
17.          }
18.          return $decrypted;
19.       }
20.    }
```

Gambar 5.3 *Source Code* Algoritme Dekripsi

Pada Gambar dijelaskan *source code* untuk melakukan proses dekripsi terhadap *ciphertext* nilai ujian setelah dilaksanakan ujian melalui perangkat *movile* peserta ujian. Fungsi algoritme Blowfish diperoleh dari *library* "mcrypt" dengan kunci yang digunakan adalah "global34blow" seperti yang telah dimasukkan pada kunci di sisi *client* (kode baris 2-3). Setelah dilakukan dekripsi maka nilai akan kembali muncul dalam wujud *plainteks* di sisi *server*.

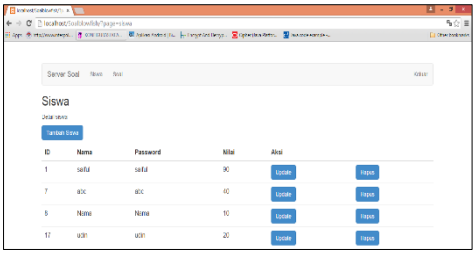
B. Implementasi Database Server

Pada implementasi database server menyediakan layanan bagi client sebagai peserta ujian online menggunakan perangkat mobile untuk menjawab soal. Diasumsikan di dalam database server telah terisi 10 soal pertanyaan mengenai permasalahan matematika dasar nantinya akan disajikan pada aplikasi ujian peserta untuk melaksanakan ujiannya seperti ditunjukkan pada Gambar 6



Gambar 4.3 Implementasi *database* soal ujian

Setelah peserta menyelesaikan pertanyaan akan menghasilkan nilai terenkripsi untuk meminimalkan resiko adanya penyadapan informasi dari pihak luar. Selanjutnya pada sisi *server* dilakukan proses dekripsi terhadap informasi nilai menggunakan kunci simetris yang sama dengan kunci dari *client* agar nilai setiap peserta yang telah melaksanakan ujian *online* dapat terbaca dalam wujud *plaintext* pada Gambar



Gambar 4.4 Implementasi Halaman Peserta

C. Hasil Pengujian Kerahasiaan

Berdasarkan hasil dari pelaksanaan ujian melalui aplikasi Android yang dilakukan dengan melibatkan 4 peserta yang telah terdaftar sebelumnya di dalam *database server*. Dengan pengumpulan hasil dari tiap peserta tersebut maka diperolehlah nilai ujian peserta beserta bentuk perlindungan fisik nilai memanfaatkan algoritme kriptografi Blowfish seperti ditunjukkan pada Tabel

Tabel 5.1 Hasil Enkripsi Nilai Peserta dengan Algoritme Blowfish

ID	Nama Peserta	Nilai Hasil	Bentuk Enkripsi	Screenshot
1	Saiful	10	cYClyop7PXS	
7	Devi	70	iYu7DYd5PII	
8	Satria	40	0BOYnm6IZSk	
17	Udin	90	QRyvfOjDMmo	

dapat dilihat bahwa nilai 4 orang peserta yang melaksanakan ujian *online* melalui aplikasi *client* dapat dilakukan enkripsi oleh sistem keamanan aplikasi dengan memanfaatkan algoritme kriptografi Blowfish. Adanya perlindungan fisik pada nilai peserta akan meningkatkan privasi atau kerahasiaan.

D. Pengujian Integritas (*Integrity*)

Pengujian integritas diperlukan untuk mengetahui apakah sistem keamanan aplikasi *client* ujian *online* memanfaatkan algoritme kriptografi Blowfish ini dapat menjaga integritas nilai peserta ujian dari upaya serangan pihak luar. Sehingga diharapkan informasi nilai peserta yang tersimpan dalam *database server* tetap utuh setelah dilakukan serangan

E. Pengujian Integritas (*Integrity*)

Pengujian integritas diperlukan untuk mengetahui apakah sistem keamanan aplikasi *client* ujian *online* memanfaatkan algoritme kriptografi Blowfish ini dapat menjaga integritas nilai peserta ujian dari upaya serangan pihak luar. Sehingga diharapkan informasi nilai peserta yang tersimpan dalam *database server* tetap utuh setelah dilakukan serangan.

V KESIMPULAN

Kesimpulan dirumuskan dan didasarkan atas hasil pengujian dan analisis yang dilakukan selama proses penelitian. Kesimpulan harus memiliki korelasi dengan rumusan masalah.Dengan kata lain, kesimpulan harus menjawab setiap poin uraian dalam rumusan masalah. Sebagai contoh,

1. Dalam sistem keamanan data dengan enkripsi blowfish pada ujian online berbasis client server data dikirimkan dari client berupa enkripsi data bukan data asli sehingga keamanan data lebih terjamin.
2. Data yang dikirimkan ke server bukan berupa data asli melainkan data enkripsi, pada server pada diubah kembali ke data aslinya untuk disimpan pada database.

Saran :

Saran berisi hal-hal yang di perlukan dalam rangka pengembangan topil skripsi selanjutnya maupun perbaikan yang harus dilakukan sesuai dengan kesimpulan yang didapatkan. Saran yang baik adalah hal-hal positif yang dapat dilakukan berdasarkan hal-hal yang menjadi temuan selama proses penelitian serta adanya manfaat atau tujuan yang mungkin bisa dicapai atau diperoleh jika saran tersebut dilaksanakan. Misalnya, "Berdasarkan hasil analisis unjuk kerja yang ada maka unjuk kerjajaringan yang sudah ada akan bisa lebih ditingkatkan dengan cara menggunakan metode re-flip-flop." atau "Pengembangan aplikasi dapat diimplementasikan lebih lanjut pada platform iOS untuk meningkatkan jumlah pengguna aplikasi dan meningkatkan popularitas aplikasi."

VI REFERENSI

[1]. [ASR-11] A. S. Rosa dan Shalahudin, M. 2011. *Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek)*. Modula, Bandung.

[2]. [CAN-01] Canavan, John E. *Fundamentals of Network Security*. 2001. London: Artech House.

[3]. [DEV-15] Developer, Android. *Built for Multiscreen World*. url: http://developer.android.com/index.html, diakses 26 September 2015.

[4]. [EMR-14] http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536. Diakses pada 21 Juni 2015.

[5]. [FAH-07] Fahmi. 2007. *Studi dan Implementasi Watermarking Citra Digital dengan Menggunakan Fungsi Hash*. Bandung: Sekolah Teknik Elektro dan Informatika. Institut Teknologi Bandung.

[6]. [FEL-12] Felker, Donn dan Burton M. 2012. *Android Application Development for Dummies*. John Wiley & Sons Inc., New Jersey.

[7]. [IBR-12] Ibrahim, Rohmat Nur. 2012. *Kriptografi Algoritma DES, AES/Rijndael, Blowfish untuk Keamanan Citra Digital dengan Menggunakan Metode Discrete Wavelet Transformation (DWT)*. Bandung: STMIK Mardira Indonesia.

[8]. [LAL-11] Laleno, B dan A. K. Taniyo. 2011. *Analisis Penggunaan Steganografi dengan Algoritma DES dan Fungsi Hash untuk Mengatasi Modifikasi Citra*. Makassar: Fakultas Teknik. Universitas Hasanuddin.

[9]. [MAT-13] Mat Jani H, dan Zughoul O. 2013. *Proposing an Encryption Algorithm Based on DES*. Malaysia: Universiti Tenaga Nasional.

[10]. [MUN-06] Munir, Rinaldi. 2006. Kriptografi. Informatika, Bandung.

VII BIODATA PENULIS

Saya lahir di Sathean 03 Januari 1992, saya anak kedua dari empat bersaudara. kakak pertama saya bernama Silvester Yogoby, ST dan nama orang tua saya Suhartono dan Serafina Fangohoi. saya memulai pendidikan saya dari TK THOMAS AQUINO Sathean, SD NASKAT Sathean, SMP PATIMURA Sathean (2004-200), SMK SIWA LIMA Langgur (2007-2010), Institut Teknologi Nasional Malang (2010-2017). Judul tugas akhir saya Sistem komunikasi full duplex untuk keamanan ujian online client-server dengan metode enskripsi algoritma blowfish mengunakan platform android dan web.

E-mail : edwardvhe061013@gmail.com