



Sistem Informasi E-Voting Berbasis Web Menggunakan Metode RSA dan Base64

Cut Lika Mestika Sandy^{*1}, Fadlisyah², Reyhan Achmad Rizal³

Email: ¹likaclms@gmail.com, ²fadlisyah@unimal.ac.id, ³reyhanachmadrizal@unprimdn.ac.id

¹Sistem Informasi, Fakultas Komputer dan Multimedia, Universitas Islam Kebangsaan Indonesia

²Sistem Informasi, Fakultas Teknik, Universitas Malikussaleh

³Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Prima Indonesia

Diterima: 23 Maret 2023 | Direvisi: 16 April 2023 | Disetujui: 30 April 2023

©2020 Program Studi Teknik Informatika Fakultas Ilmu Komputer,
Universitas Muhammadiyah Riau, Indonesia

Abstrak

Permasalahan saat ini yang sedang dihadapi oleh Desa Gampong Cot Girek Kandang Aceh Utara yaitu pemilihan Keuchiek masih dilakukan secara manual. Pemilihan secara manual memiliki banyak kendala salah satunya yaitu rentan akan kecurangan hasil pemungutan suara dikarenakan hasil tidak dapat ditampilkan secara realtime. Selain itu juga banyak pemilih yang tidak ikut memilih dikarenakan administrasi dalam pemilihan yang tidak efisien, sehingga dalam pemilihan keuchiek dibutuhkan suatu sistem yang dapat menyelesaikan permasalahan tersebut. Berdasarkan permasalahan tersebut pada penelitian ini akan diusulkan sistem pemilihan secara online dengan e-voting berbasis web. Sistem e-voting berbasis web pada penelitian ini dibuat menggunakan metode kriptografi RSA dan Base64 untuk mengamankan data hasil pemungutan suara dan model pengembangan sistem yang digunakan menggunakan model SDLC air terjun (waterfall). Metode pengujian sistem yang digunakan adalah Black box, pengujian dilakukan oleh 120 orang yang meliputi: user admin, user pengguna dan peserta calon keuchiek. Hasil penelitian menunjukkan sistem e-voting berbasis web menggunakan RSA dan Base64 sangat baik digunakan dalam pemilihan Keuchiek selain menghemat biaya dikarenakan tidak membutuhkan petugas terlalu banyak serta dapat meningkatkan minat masyarakat didalam melakukan pemilihan.

Kata kunci: Keuchiek, RSA, Base64

Web-Based E-Voting Information System Using RSA and Base64 Methods

Abstract

The current problem being faced by Gampong Cot Girek Kandang North Aceh Village is that the selection of Keuchiek is still done manually. Manual selection has many obstacles, one of which is being vulnerable to fraud in voting results because the results cannot be displayed in real-time. In addition, many voters do not vote due to inefficient election administration, so in the election of keuchiek a system is needed that can solve this problem. Based on these problems, this research will propose an online voting system with web-based e-voting. The web-based e-voting system in this study was created using the RSA and Base64 cryptographic methods to secure voting results data and the system development model used was the waterfall SDLC model. The system testing method used is the Black box, the test was carried out by 120 people including admin users, user users and prospective keuchiek participants. The results of the study show that a web-based e-voting system using RSA and Base64 is very good for use in Keuchiek elections besides saving costs because it does not require too many officers and can increase public interest in conducting elections.

Keywords: Keuchiek, RSA, Base64

1. PENDAHULUAN

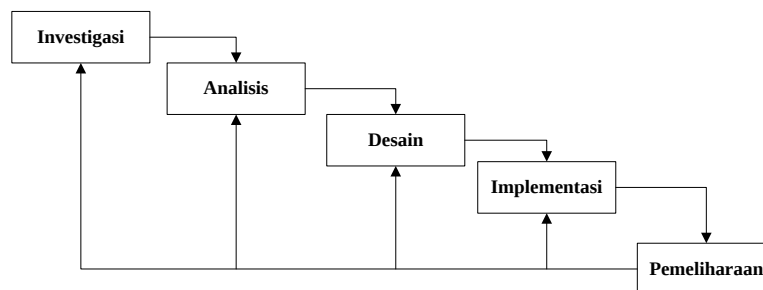
Pemilihan *keuchiek* merupakan kegiatan yang dilakukan setiap lima tahun sekali untuk pergantian masa jabatan. Saat ini proses kegiatan pemilihan *keuchiek* Desa di Gampong Cot Girek Kandang Aceh Utara masih dilakukan secara konvensional sehingga prosesnya terlalu menyulitkan untuk pemilihan serta dana yang harus dikeluarkan juga cukup besar. Pemilihan secara konvensional saat ini juga rentan akan kecurangan hasil suara dikarenakan banyak masyarakat yang memiliki hak untuk memilih tidak ikut memilih dikarenakan administrasi yang menyulitkan. Pemilihan dengan memanfaatkan teknologi sebagai medianya

sudah banyak dilakukan di beberapa daerah. Salah satunya teknologi yang sering digunakan yaitu dengan menggunakan sistem *e-voting*, dengan *e-voting* semua proses dari pendaftaran peserta hingga pemungutan suara dilakukan secara digital. *E-voting* merupakan sistem yang dapat membantu proses pemungutan dan penghitungan suara menjadi lebih efisien dan menghemat biaya pada saat pemilihan umum dilakukan. Berdasarkan permasalahan tersebut desa Gampong Cot Girek Kandang Aceh Utara membutuhkan teknologi yang dapat digunakan pada saat pemilihan *keuchiek*. Sistem pemilihan yang diusulkan pada penelitian ini yaitu pemilihan secara online atau *e-voting* berbasis web. Sistem *e-voting* dibuat dengan memanfaatkan *kriptografi* didalam mengamankan data pemilihan suara. Metode *kriptografi* yang digunakan pada sistem *e-voting* yaitu RSA dan *base64*. Beberapa penelitian mengenai penerapan kriptografi pada sistem *e-voting* yaitu :[1] Pada penelitiannya untuk mengamankan data pemilihan menggunakan *RFID* dan metode RSA hasilnya tingkat keberhasilan dari proses enkripsi dan dekripsi sebesar 100%. Penelitian serupa juga dilakukan oleh [2] dimana dalam mengamankan data pada sistem *e-voting* menggunakan metode RSA. Selanjutnya penelitian dilakukan oleh [3] Pada penelitiannya menerapkan metode RSA dan *base64* dalam mengamankan data *e-voting* pengujian dilakukan dengan *korelasi*, *entropy* dan waktu enkripsi hasilnya pengamanan *database* dengan enkripsi RSA dan *base64* sangat bagus.

2. METODE PENELITIAN

2.1 Metode pengembangan sistem

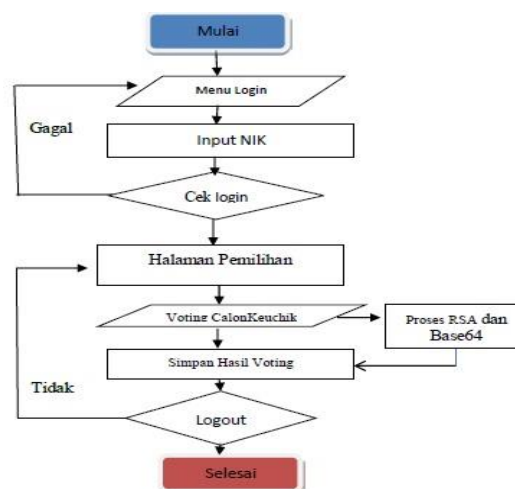
Metode pengembangan sistem yang digunakan dalam peneltian ini menggunakan model *SDLC air terjun (waterfall)*. Tahapan pengembangan dapat dilihat pada gambar 1.



Gambar 1 Skema waterfall[4][5][6][7]

Pada gambar 1 dapat dilihat model yang akan digunakan dalam pengembangan sistem. Dimulai dengan melakukan ivestigasi untuk menentukan apakah yang menjadi permasalahan sebelumnya. Selanjutnya melakukan analisis sistem untuk mengetahui kebutuhan sistem yang akan dibangun dan setelah mendapatkan data-data yang dibutuhkan akan dilanjutkan pada tahapan desain sistem. Pada tahap ini ilustrasi sistem yang akan dibangun diilustrasikan dengan Flowchart sebagai model alur sistem dan *ERD* (*Entity Relationship Diagram*) sebagai rancangan model relasi antar database. Selanjutnya pada tahap implementasi menggunakan bahasa pemrograman *PHP* dan *HTML* serta *CSS* untuk mendesain tampilan web. Tahap akhir yaitu tahapan pemeliharaan dilakukan ketika sistem informasi sudah dioperasikan. Pada tahapan ini dilakukan monitoring proses, evaluasi dan perubahan (perbaikan) bila diperlukan.

2.2 Desain aplikasi



Gambar 2. Tahap Pengembangan Aplikasi[8][9][10][11]

Gambar 2 menggambarkan dalam penelitian membuat aplikasi e-voting pemilihan pemilihan *keuchiek* Desa di Gampong Cot Girek Kandang aceh utara diawali dengan memasukan nik, jika nik yang ditulis terdaftar di database maka password akan dikirimkan melalui email, dan anggota akan diarahkan ke form halaman pemilihan untuk memilih calon *keuchiek* selanjutnya data akan diproses menggunakan *RSA* dan *Base64* dan data akan disimpan di dalam database.

2.3. Implementasi Algoritma *RSA*[12][13][14]

Contoh untuk implementasi algoritma *RSA*:

1. Ambil nilai dari plaintext yaitu $x = 148$
2. Ubah plainteks tersebut kedalam bentuk ASCII Code sehingga menjadi 495256, dimana $1 = 49$, $4 = 52$, $8 = 56$
3. Kemudian ambil kunci publik yaitu (2089, 8591159), berarti $e = 2089$ dan $n = 8591159$
4. Lakukan perhitungan dengan rumus = seperti dibawah ini:

$$4952562089 \bmod 8591159 = 7967745$$

Jadi ciphertext yang dihasilkan adalah

$$Y = 7967745$$

2.4. Implementasi *RSA* dengan Algoritma *Base64*[15]

Langkah-langkah enkripsi dari *Base64*, jika sebuah string (bytes) yang akan disandikan ke algoritma *base64* maka tahapannya yaitu:

1. Hitung panjang karakter yang akan kita enkripsi. kemudian jumlah karakter dikali 8.
2. Hasil dari tahap pertama kemudian dibagi 6.
3. Ambil nilai binary dari setiap huruf yang akan di enkripsi;
4. Kemudian sejajarkan angka binary dari setiap huruf tersebut.
5. Kemudian ubah menjadi binary yang awalnya 8 bit menjadi binary berukuran 6 bit dalam blok ukuran 6 bit.
6. Hitung angka biner 6 bit tersebut dan ubah ke dalam bentuk decimal.
7. Ubah bentuk decimal ke dalam bentuk karakter berdasarkan tabel enkripsi *base64*.

Catatan apabila panjang karakter bukan merupakan kelipatan 3 atau dalam pembagian hasil bilangan menjadi 6 bit ada sisa pembagi, maka ditambahkan karakter pad (=) sebagai penggenap. Oleh karena itu, terkadang pada *Base64* akan muncul satu atau dua karakter(=).

3. HASIL DAN PEMBAHASAN

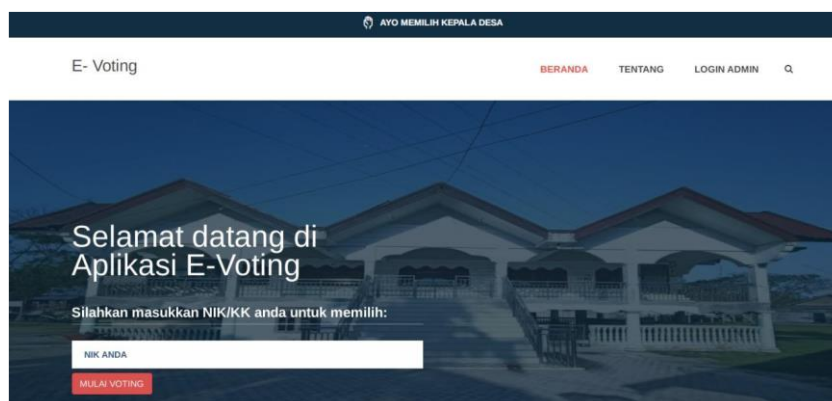
3.1 Halaman login



Gambar 3. Tampilan Halaman login admin

Pada gambar 3 merupakan halaman login admin sistem e-voting dimana ketika admin mengakses masuk sebuah sistem pengguna diharapkan memasukan username dan password. Kemudian sistem akan memvalidasi apakah sudah benar, jika benar maka akan lanjut ke halaman beranda atau halaman utama.

3.2 Tampilan Halaman Login Pemilih



Gambar 4. Tampilan Halaman login pemilih

Gambar 4 merupakan halaman utama pemilih, pada halaman ini berisi informasi singkat tentang tata cara pemilihan bagaimana pemilih memberikan suara atau pilihannya kepada calon kandidat *Keuchiek*. Pemilih diwajibkan mengisi NIK yang sebelumnya sudah dibuatkan dari admin untuk bisa masuk dan melakukan pemilihan melalui sistem.

3.3 Tampilan Halaman Beranda



Gambar 5. Tampilan Halaman Beranda

Gambar 5 merupakan halaman utama atau halaman beranda tampilan pertama admin yang akan tampil ketika admin berhasil login setelah dilakukan verifikasi oleh sistem. Di dalam halaman utama ini terdapat fungsi – fungsi penunjang dari sistem e-voting ini antara lain pengelolaan input calon ketua atau kandidat, pengelolaan data pemilih, daftar DPT, data dusun dan laporan hasil suara pemilihan

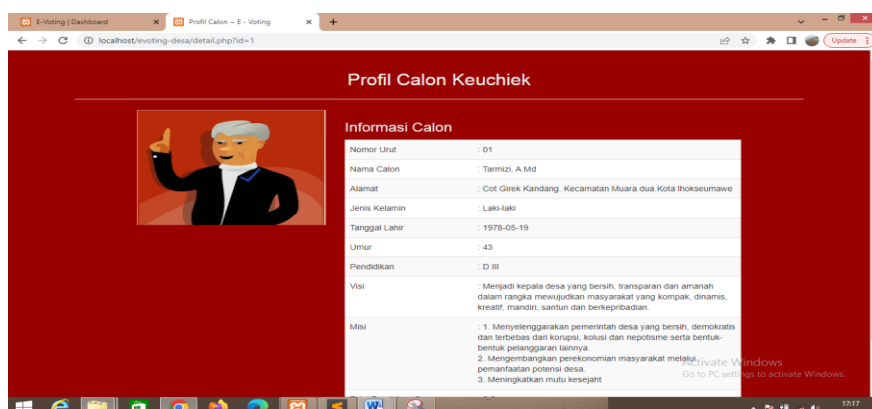
3.4 Tampilan Halaman Pemilihan



Gambar 6. Tampilan Halaman Pemilihan

Gambar 6. merupakan halaman pemilihan pada tampilan halaman ini berisi foto calon kandidat dan fungsi lihat visi dan misi calon kandidat. Fungsi utama dari halaman ini adalah masukan atau inputan suara yang dipilih oleh pemilih kemudian data tersebut akan dikumpulkan dan bersumber di database sistem.

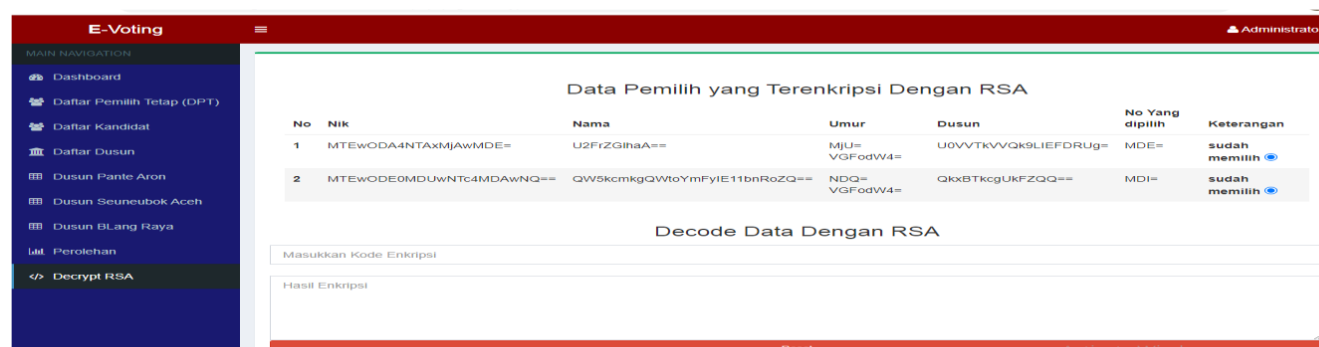
3.5 Tampilan Halaman Visi dan Misi



Gambar 7. Tampilan Halaman Visi Misi

Gambar 7 merupakan halaman visi dan misi kandidat, Pemilih dapat Melihat visi dan misi calon kandidat keuchik serta melihat profil kandidat secara detail

3.6 Tampilan Halaman Logout



Gambar 8. Tampilan Enkripsi RSA

Gambar 8 merupakan tampilan Decrypt RSA disinilah data pemilih akan terenkripsi otomatis oleh sistem dan bisa juga deskripsi kembali juga jika memang perlu dan ini hanya bisa dikelola oleh admin saja.

3.7 Hasil Pengujian Sistem

Untuk mengetahui keberhasilan penerapan sistem yang telah dilakukan, maka perlu dilakukan pengujian terhadap sistem tersebut. Metode pengujian yang digunakan adalah Black box, pengujian dilakukan oleh admin, pengguna(masyarakat), peserta calon keuchiek. Tahapan pengujian yang telah dilakukan adalah sebagai berikut:

Tabel 1. Pengujian sistem e-voting pemilihan calon keuchiek

No	Keterangan	Prosedur	Inputan	Ouput	Hasil	Kesimpul an
1	Pengujian masuk sistem	halaman masuk	Isi username "staf45" dan password "12345"	Masuk ke sistem (halaman tambah pemilih)	Masuk ke sistem	Bagus
2	Pengujian masuk sistem	halaman masuk	Isi username "staf45" dan password "12345"	Masuk ke sistem (halaman tambah kandidat)	Masuk ke sistem	Bagus
3	Menguji edit data pemilih	Buka halaman tambah	Ubah dan tambah NIK, nama warga,	Perubahan data pada halaman pemilih	Perubahan data pada	Bagus

		pemilih dan klik edit pada data pemilih	tanggal lahir, umur, jenis kelamin, dusun.		halaman pemilih	
4	Menguji edit data kandidat	Buka halaman tambah kandidat dan klik edit pada data kandidat	Ubah dan tambah Nama kandidat, nik, alamat, jenis kelamin, tanggal lahir, umur, pendidikan, foto kandidat, visi dan misi	Perubahan data pada halaman kandidat	Perubahan data pada halaman kandidat	Bagus
5	Menguji edit data Dusun	Buka halaman tambah Dusun dan klik edit pada data dusun	Ubah dan tambah Nama dusun	Perubahan data pada halaman kandidat	Perubahan data pada halaman kandidat	Bagus
6	Menguji data perolehan suara	Buka halaman perolehan suara	Data ditampilkan	Data ditampilkan	Data ditampilkan	Bagus
7	Menguji data enkripsi RSA dan Base64	Buka halaman enkripsi RSA	Data terenkripsi	Data terenkripsi	Data terenkripsi	Bagus

4. KESIMPULAN

Berdasarkan hasil pengujian yang sudah dilakukan penerapan sistem e-voting pemilihan *Keuchiek* Desa di Gampong Cot Girek Kandang Aceh Utara pengujian berjalan lancar tanpa kendala error dengan total 100 data input selama pengujian. Permasalahan seperti proses yang terlalu menyulitkan untuk melakukan pemilihan dapat terselesaikan dan masyarakat dapat melakukan pemilihan tanpa harus ke tempat pemilihan sehingga mampu meningkatkan masyarakat untuk melakukan pemilihan. Sistem e-voting pada penelitian ini memiliki tingkat keamanan yang cukup baik dimana satu warga hanya boleh menggunakan satu Nik untuk melakukan pemilihan. Pengamanan data suara juga menggunakan algoritma RSA dan base 64 pada saat pemilih melakukan voting.

DAFTAR PUSTAKA

- [1] A. S. Indrawanti, A. W. Azinar, and M. A. Firdiansyah, "Secure E-Voting Menggunakan Metode Rsa Dan Autentikasi Rfid," *Netw. Eng. Res. Oper.*, vol. 4, no. 1, pp. 67–75, 2018, doi: 10.21107/nero.v4i1.113.
- [2] B. Fitrianto Wibowo *et al.*, "E-Voting Application Using RSA Algorithm Method Based Prototype Android," *J. Tek. Inform. C.I.T.*, vol. 11, no. 1, pp. 8–14, 2019, [Online]. Available: www.medikom.iocspublisher.org/index.php/JTI
- [3] S. Kasus, P. Presiden, and M. Stmik, "Implementasi Kriptografi Dalam Pengamanan Database E-Voting Menggunakan Algoritma Rsa Dan Base64 Berbasis Progresive Web Apps," *e-Jurnal JUSITI (Jurnal Sist. Inf. dan Teknol. Informasi)*, vol. 10, no. 1, pp. 30–40, 2021, doi: 10.36774/jusiti.v10i1.818.
- [4] Norhayati, Rosmiati, V. Zefanya, and C. Elmayantie, "Rancangan aplikasi reading comprehension berbasis web," vol. 3, no. 3, pp. 371–381, 2022.
- [5] Darmanta Sukrianto and Sinta Maria, "Implementasi Sistem Informasi Repository Tugas Akhir Pada Amik Mahaputra Riau Berbasis Web," *J. CoSciTech (Computer Sci. Inf. Technol.)*, vol. 3, no. 3, pp. 350–357, 2022, doi: 10.37859/coscitech.v3i3.4362.
- [6] M. Analisis and S. Share, "Jurnal Computer Science and Information Technology (CoSciTech) Perancangan Sistem Informasi Sektor Ekonomi Unggulan Provinsi Sulawesi Selatan Design of Leading Economic Sector Information Systems for South Sulawesi Province Using LQ Analysis and Shift S," vol. 3, no. 3, pp. 325–330, 2022.
- [7] P. Studi, S. Informasi, F. Komputer, and U. I. Batam, "Jurnal Computer Science and Information Technology (CoSciTech) Analisis perbandingan Codeigniter dan Yii framework pada perancangan website rencana anggaran biaya Comparative analysis of Codeigniter and Yii framework on website design budget plans," vol. 3, no. 3, pp. 249–258, 2022.
- [8] M. Ula, R. R. Mutuahmi, S. Fachrurrazi, R. A. Rizal, and I. Sahputra, "Aplikasi Sistem Informasi Geografis Pencarian Rumah Sakit dan Puskesmas dengan Algoritma Djikstra Berbasis Android," vol. 10, no. 1, pp. 348–355, 2023, doi: 10.30865/jurikom.v10i1.5609.
- [9] S. N. Husna, M. Ula, and R. A. Rizal, "APLIKASI PENGEMBANGAN TECHNOPRENEUR MELALUI APLIKASI SMART TRANSPORTATION SYSTEM MENGGUNAKAN ALGORITMA A * DALAM," vol. 7, no. 1, pp. 227–232, 2023.
- [10] Johny Soetikno, S. Aisa, Reza Selviana, and Gusti Fernando, "Implementasi Metode Single Moving Average pada Aplikasi Order Indent Berbasis Web," *J. CoSciTech (Computer Sci. Inf. Technol.)*, vol. 3, no. 3, pp. 291–299, 2022, doi: 10.37859/coscitech.v3i3.4235.
- [11] F. Muttakin, D. Dwi Aprilia, and M. Kumalasari, "Analisis Pengaruh Kualitas Layanan Website Terhadap Pengguna Akhir Menggunakan Webqual 4.0," *J. CoSciTech (Computer Sci. Inf. Technol.)*, vol. 3, no. 3, pp. 300–308, 2022, doi: 10.37859/coscitech.v3i3.4403.
- [12] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 6, no. 1, pp. 1–10, 2019, doi: 10.33330/jurteks.v6i1.395.
- [13] K. Edwin, H. Christinal, and A. Chandy, "EasyChair Preprint № 7407 Blockchain Based Online Voting System Using RSA Algorithm," 2022.



- [14] Na. Sundar and A. Professor, "A Secure E-Voting System Using RSA and Md5 Algorithms Using Random Number Generators," *Int. J. Appl. Eng. Res.*, vol. 13, no. 11, pp. 9468–9473, 2018, [Online]. Available: <http://www.ripublication.com>
- [15] F. Febriyanto, "Rancang Bangun Website Kriptografi Untuk Pengamanan File Gambar Digital," *J. Khatulistiwa Inform.*, vol. 10, no. 2, pp. 113–118, 2022, [Online]. Available: <https://ejournal.bsi.ac.id/ejurnal/index.php/khatulistiwa/article/view/14432%0Ahttps://ejournal.bsi.ac.id/ejurnal/index.php/khatulistiwa/article/viewFile/14432/5711>