

IMPLEMENTASI ALGORITMA BLOWFISH PADA SISTEM MANAJEMEN SURAT DENGAN PENDEKATAN RATIONAL UNIFIED PROCESS YANG RAMAH LINGKUNGAN

Filan Firmansyah¹, Saputra Dwi Nurcahya², Zuhana Realita Alfy³

^{1,2,3} Fakultas Teknik dan Ilmu Komputer, Universitas Indraprasta PGRI, Jakarta, Indonesia

¹filanfirmsyah20@gmail.com

²saputra.dwinurcahya@unindra.ac.id

³zuhanarealita28@gmail.com

Abstract

In many organizations, including the Institut Teknologi Perusahaan Listrik Negara (ITPLN), letter management and organization is very important. This process is often resource-intensive and time-consuming. With the advancement of information technology, a secure digital system can help optimize letter management. The implementation of Blowfish cryptographic algorithm for encryption of important data on letter stored in a digital-based letter management system is the subject of this research. This method lowers the potential for eavesdropping and data theft. In the development process of this system, the Rational Unified Process (RUP) methodology takes the principle of green computing, which helps improve the efficiency of environmental destruction. The system adopts a paperless office paradigm, addresses the issue of operational inefficiencies, and safeguards sensitive data. The Blowfish algorithm prevents irresponsible people from compromising the database. This research produces a secure letter management information system using blowfish algorithm and developed using RUP that is environmentally friendly in contribution to the efficiency of environmental destruction caused by software development.

Keywords: Blowfish Algorithm, Rational Unified Process, Data Security, Letter Management, Eco-Friendly Software

I. PENDAHULUAN

Surat hampir digunakan dalam setiap kegiatan perusahaan atau institusi di Indonesia. Ini karena surat adalah alat komunikasi yang penting untuk menyampaikan informasi secara tertulis. Dalam hal ini, pengelolaan dan manajemen korespondensi sangat penting. Akibatnya, proses ini harus mendapat perhatian lebih untuk memastikan bahwa bisnis atau lembaga berjalan dengan baik (Suparmadi dkk., 2024). Setiap bagian dari suatu organisasi harus mengikuti prosedur pengelolaan dan manajemen surat, yang mencakup penomoran, pembuatan, pendataan, dan pengarsipan [1].

Di Institut Teknologi Perusahaan Listrik Negara (ITPLN), proses ini dilakukan dengan mengatur penomoran surat melalui satu pintu, Bagian Administrasi Umum (BAUM), dan pengarsipan surat sambil menyimpan berkas fisik surat pada binder. Akibatnya, proses pengelolaan dan manajemen surat sering memakan waktu yang lama karena pejabat yang berwenang tidak berada di tempat atau melakukan kesalahan pada tanda tangan mereka. Selain memakan waktu yang lama, hal ini juga menghabiskan banyak kertas dan tinta yang digunakan untuk menulis. Selain itu, menghubungi pegawai BAUM terlebih dahulu untuk menyelesaikan surat yang dibuat di luar jam kerja seringkali memakan waktu yang lebih lama.

Dengan pesatnya kemajuan teknologi informasi dan sistem informasi dalam hampir semua aspek kehidupan modern,

kemajuan ini dapat dimanfaatkan untuk menyelesaikan masalah yang mungkin terjadi dalam proses pengelolaan dan manajemen surat [1]. Di era modern, komunikasi digital dapat mengakibatkan penyadapan, penyalahgunaan, dan pencurian data sensitif oleh pihak yang tidak berwenang. Apalagi jika data pribadi tersebar di seluruh perusahaan. Oleh karena itu, sangat penting untuk memastikan bahwa data yang disimpan aman. Semua surat masuk dan keluar yang dikirim ke sekolah harus disimpan rahasia. Ini termasuk lokasi pengiriman dan asal usul [2]. Kriptografi blowfish adalah salah satu dari banyak teknik penyandian yang ada saat ini, yang menggunakan blok cipher 64 bit dengan panjang kunci yang dapat diubah [3].

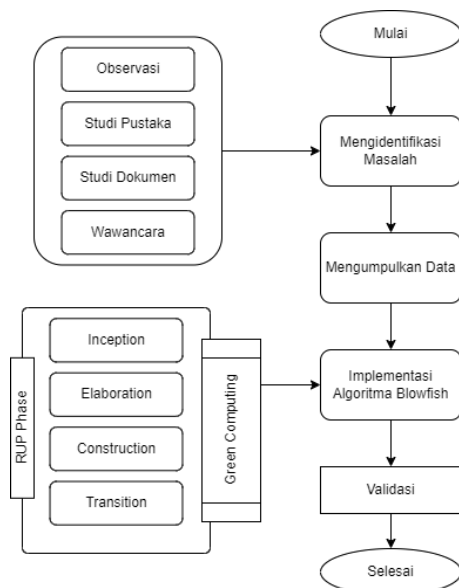
Mengatasi masalah yang mendesak membutuhkan pendekatan yang inovatif dan berkelanjutan dalam menghadapi tantangan yang terus berkembang. Tujuan penelitian multidisipliner ini adalah untuk mengatasi perbedaan yang signifikan di berbagai aspek. Fokusnya mencakup sejumlah masalah penting, termasuk efek pemanasan global yang meningkat yang disebabkan oleh penggunaan teknologi yang tidak efisien [4], rencana untuk melindungi data sensitif aplikasi melalui penggunaan algoritma [3], penjadwalan dan manajemen sertifikasi asisten dan kepala laboratorium yang tidak efisien [5], metamorfosis yang signifikan dari sistem penjualan manual ke sistem berbasis web [6], potensi transformatif dalam mengadopsi paradigma kantor tanpa kertas [7], masalah dengan pencarian arsip surat [1] dan pertimbangan

yang cermat terhadap metodologi pengembangan perangkat lunak [8] Setiap komponen dianalisis secara menyeluruh, menghasilkan kesimpulan yang relevan, dan menawarkan solusi yang berguna.

Pada penelitian ini, algoritma blowfish digunakan untuk melakukan enkripsi data penting pada surat yang tersimpan dalam database melalui sistem manajemen surat. Ini dilakukan untuk mencegah pihak tidak bertanggung jawab untuk merusak database sebagaimana yang dilakukan oleh [2]. Studi ini mengembangkan sistem manajemen surat yang menggunakan metodologi Rational Unified Process (RUP) yang ramah lingkungan. Metodologi ini juga mempertimbangkan prinsip komputasi hijau, sehingga perangkat lunak yang dihasilkan juga dapat membantu meningkatkan efisiensi perusahaan lingkungan sebagaimana yang dikemukakan oleh [9] dalam penelitiannya. Selain itu, penggunaan Algoritma Blowfish memastikan bahwa data penting yang dimasukkan ke dalam sistem ketika disimpan pada database lebih aman.

II. METODOLOGI PENELITIAN

Sebagai solusi dari permasalahan yang dihadapi di ITPLN terkait dengan optimasi manajemen surat pada beberapa proses yaitu waktu yang dibutuhkan dalam pengelolaan surat, pengelolaan dan manajemen arsip, penggunaan sumber daya seperti tinta dan kertas serta keamanan pada data surat yang disimpan secara digital dibuatlah sistem informasi manajemen surat yang mengadopsi algoritma blowfish sebagai keamanan pada data surat yang disimpan secara digital dan dikembangkan menggunakan metodologi RUP yang ramah lingkungan sebagai kontribusi terhadap efisiensi perusahaan lingkungan yang disebabkan oleh pengembapngan perangkat lunak. Langkah-langkah yang dilakukan dalam penelitian ini secara lengkap tersaji pada gambar 1.



Gambar 1. Desain Penelitian

Metodologi RUP yang mengadaptasi prinsip-prinsip green computing digagas oleh [9] dengan mengintegrasikan tahapan RUP yang dikembangkan oleh international business machines corporation (IBM) dengan prinsip green computing sehingga menghasilkan luaran yang berkontribusi terhadap program skala global yaitu sustainable development goals (SDGs). Matrix RUP ramah lingkungan yang digagas oleh [9] tersaji pada tabel 1.

Tabel 1. Dokumen Luaran RUP

RUP Phases			
Inception	Elaboration	Construction	Transition
System Charter	Software requirement specification	Software development result	Software test report and user acceptance test

Algoritma kriptografi blowfish dipilih sebagai penyandian atau enkripsi pada data sensitif surat karena dilansir dari [3] pada penelitiannya yang membandingkan algoritma rivest-shamir-adleman (RSA) dan blowfish keamanan data mendapat Kesimpulan bahwa data yang di enkripsi menggunakan blowfish memakan waktu lebih lama untuk di dekripsi dibandingkan dengan data yang di enkripsi dengan RSA.

Sitinjak dalam [10] menjelaskan bahwa Algoritma blowfish, yang dikembangkan oleh Bruce Schneier, dimaksudkan untuk digunakan pada mikroprocessor besar yang memiliki chace data yang besar. Metode ini mirip dengan metode data encryption standard (DES). Algoritma Blowfish terdiri dari dua bagian: penambahan kunci dan enkripsi data. Chipper blok Blowfish memiliki panjang kunci yang berbeda-beda. Dengan menggunakan key expansion, Anda dapat mengubah satu kunci hingga 448 bit ke dalam beberapa array sub-key yang memiliki total 4168 byte. Enkripsi data terdiri dari sebuah fungsi sederhana yang melakukan 16 iterasi. Setiap iterasi memiliki permutasi yang bergantung pada tombol, berganti tombol, dan bergantung pada data. Hanya ada operasi penambahan di indeks empat lookup data array per round, dan semua operasi, penjumlahan, dan XOR pada kata 32 bit. Sebelum enkripsi atau dekripsi, Anda harus menghitung banyak subkey Blowfish. [3].

Menurut Schneier dalam [2], Alur algoritma yang dienkripsi melalui metode blowfish adalah sebagai berikut:

- Array P memiliki bentuk awal 18 buah (P1, P2,..., P18) yang masing-masing memiliki nilai 32 bit. Array P terdiri dari delapan belas subkunci bernilai 32 bit: P1, P2,..., P18.
- Empat S-box bernilai 32 bit masing-masing memiliki 256 masukan. Empat S-box bernilai 32 bit masing-masing memiliki 256 masukan:
S1, 0, S1, 1,, S1, 255
S2, 0, S2, 1,, S2, 255
S3, 0, S3, 1,, S3, 255
S4, 0, S4, 1,, S3, 255

- c) Plaintext yang akan dienkripsi dianggap sebagai masukan; bitnya diambil sebanyak 64 bit, dan jika ada bit yang kurang dari 64 bit, bit tersebut dapat ditambahkan untuk memastikan bahwa datanya nanti sesuai dengan operasinya.
- d) Hasil pengambilan 32 bit dibagi menjadi dua: yang pertama disebut XL, dan yang kedua disebut XR.
- e) Kemudian selesaikan operasi $XL = XL \text{ XOR } P_i$ dan $XR = F(XL) \text{ XOR } XR$.
- f) Operasi tersebut mengubah XL menjadi XR dan XR menjadi XL.
- g) Sekali lagi, lakukan proses penukaran XL dan XR pada perulangan ke-16.
- h) Operasi dilakukan untuk $XR = XR \text{ XOR } P_{17}$ dan $XL = XL \text{ XOR } P_{18}$.
- i) Proses terakhir satukan kembali XL dan XR sehingga kembali menjadi 64 bit.

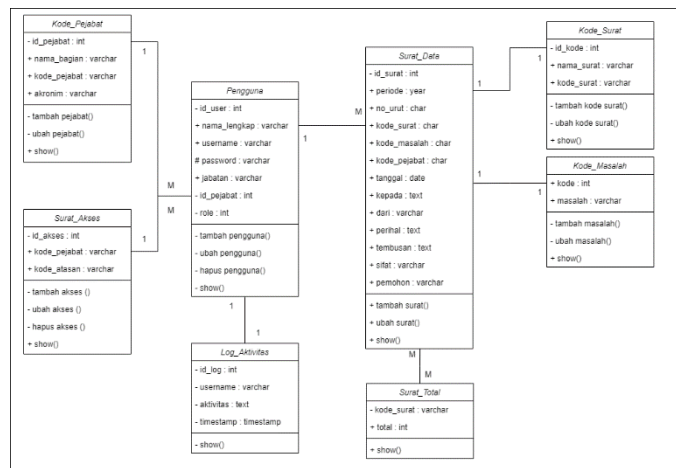
Dalam pengembangannya, sistem informasi manajemen surat dikembangkan menggunakan bahasa pemrograman hypertext preprocessor (PHP) yang mana dalam melakukan enkripsi sudah dilengkapi dengan salt. Dilansir dari [11] enkripsi yang dilengkapi dengan salt tingkat keamanannya bertambah, dikarenakan dengan plain text dan kunci enkripsi yang sama dapat menghasilkan cipher text yang berbeda.

III. HASIL DAN PEMBAHASAN

Dalam memberikan solusi terhadap berbagai permasalahan yang ada dalam proses manajemen surat di ITPLN, dilakukan beberapa tahapan yaitu :

A. Analisa Basis Data

Berdasarkan identifikasi masalah dan pengamatan yang dilakukan penulis terhadap proses manajemen surat di ITPLN, didapatkan apa-apa saja data yang akan disimpan secara digital melalui sistem informasi manajemen surat yang akan dibuat. Data ini tersaji dalam bentuk class diagram pada gambar 2.



Gambar 2. Class Diagram

B. Analisa Tingkat Kesensitifan Data

Analisa tingkat kesensitifan data dilakukan untuk menentukan data atau bagian mana pada surat berdasarkan class diagram yang harus diamankan atau dilakukan enkripsi ketika disimpan secara digital.

Analisa ini dilakukan dengan gap analysis pada beberapa sumber terkait yang dicari menggunakan kata kunci (“surat” AND “Enkripsi”) pada laman google scholar dengan batas publikasi tahun 2020. Hasil analisa yang dilakukan tersaji secara detil pada tabel 2.

Tabel 2. Analisa Tingkat Kesensitifan Data

Penulis (Tahun)	DOI/Link	Bagian yang di enkripsi
Implementasi algoritma Caesar cipher dan algoritma RSA untuk keamanan data surat wasiat pada kantor notaris/PPAT Robert Tampubolon, S.H. [12]	https://sostech.greenvest.co.id/index.php/sostech/article/view/64/718	Isi Surat
Pengujian keamanan komputer kriptografi pada surat elektronik berbasis web dengan enkripsi metode MD5 [13]	https://doi.org/10.52362/jmijayakarta.v1i1.367	Pemohon, Pengirim dan Penerima Surat
The implementation of modern cryptography on document data security [14]	https://doi.org/10.37676/jmcs.v1i2.2742	Isi Surat
Penerapan digital signature untuk persuratan dengan menggunakan metode algoritma SHA1 di sektor pertanian, ketahanan pangan dan perikanan Kab. Mempawah [15]	http://jurnal.kolibi.org/index.php/scientifica/article/view/1196/1130	Tandatangan Digital
Penerapan metode elgamal untuk mengamankan teks pada file dokumen word [16]	http://djournals.com/klik/article/view/1277/786	Isi Surat
Implementasi algoritma SHA512 pada	https://journal-computing.org/index.php/journal-	Nama File Surat

keamanan berita ita/article/view/349/
acara hasil sidang 159
berbasis web [17]

Berdasarkan analisa yang telah dilakukan sesuai dengan tabel 2, didapatkan hasil bahwa tiga dari enam best practice melakukan enkripsi dan peningkatan keamanan pada isi dari surat. Sehingga, berdasarkan hal tersebut didapatkan bagian yang dapat dikatakan sebagai bagian paling sensitif pada sebuah surat yaitu isi surat.

C. Inisiasi Penerapan Algoritma Blowfish

Untuk mengimplementasikan algoritma blowfish ke dalam sistem manajemen surat yang telah dikembangkan, diperlukan beberapa konfigurasi pada framework pengembangan. Konfigurasi dan inisiasi dilakukan sebagai berikut:

- 1) Inisiasi yang pertama kali dilakukan adalah memanggil library enkripsi yang mana akan digunakan untuk pemanggilan enkripsi pada proses pengkodean, tersaji pada gambar 3.

```
58 $autoload['libraries'] = array('user_agent' => 'ua');  
59 */  
61 $autoload['libraries'] = array('database', 'session', 'encryption');  
62
```

Gambar 3. Pemanggilan Library

- 2) Selanjutnya dilakukan pemanggilan blowfish pada enkripsi yang dilakukan, karena jika hal ini tidak dilakukan enkripsi akan menggunakan algoritma secara acak yang tersedia pada library yang telah dipanggil sebelumnya seperti terlihat pada gambar 4.

```
// Menginisialisasi library enkripsi dengan cipher 'blowfish'  
$this->encryption->initialize(array('cipher' => 'blowfish'));
```

Gambar 4. Inisiasi Library

- 3) Langkah berikutnya adalah menentukan kunci enkripsi sebagai key untuk melakukan enkripsi dan dekripsi menggunakan blowfish seperti terlihat pada gambar 5.

```
Encryption Key  
-----  
If you use the Encryption class, you must set an encryption key.  
See the user guide for more info.  
  
https://codeigniter.com/user_guide/libraries/encryption.html  
*/  
$config['encryption_key'] = 'itpln';
```

Gambar 5. Penetapan Kunci Enkripsi

- 4) Setelah semua inisiasi dan konfigurasi dilakukan, barulah dapat dilakukan implementasi algoritma blowfish pada sistem manajemen surat yang dikembangkan dalam penelitian ini.

D. Implementasi Algoritma Blowfish pada Sistem Manajemen Surat

- 1) Pertama-tama dilakukan implementasi untuk enkripsi isi surat yang mana sesuai dengan kebutuhan, isi dari surat yang disimpan pada database adalah bagian perihal ketika diinputkan melalui isian yang terdapat pada sistem manajemen surat seperti terlihat pada gambar 6.

```
$hal = $this->input->post('perihal', TRUE);  
$perihal = $this->encryption->encrypt($hal);
```

Gambar 6. Enkripsi Isian

- 2) Setelah dilakukan implementasi algoritma blowfish pada hasil masukkan, barulah data tersebut dapat disimpan ke database seperti terlihat pada gambar 7.

```
$data = array(  
    'no_urut' => $no_urut,  
    'periode' => date('Y'),  
    'kd_surat' => $this->input->post('surat', TRUE),  
    'kd_masalah' => $this->input->post('masalah', TRUE),  
    'kd_jabatan' => $kd_pejabat->kode,  
    'tahun' => $this->input->post('tahun', TRUE),  
    'tanggal' => date('Y-m-d'),  
    'kepada' => $kepada,  
    'dari' => $this->input->post('pejabat', TRUE),  
    'perihal' => $perihal,  
    'amplop' => $amplop,  
    'tambahan' => $tambahan,  
    'pemohon' => $this->input->post('pemohon', TRUE),  
    'sifat' => $this->input->post('sifat', TRUE),  
    'ket' => $this->input->post('ket', TRUE),  
);
```

Gambar 7. Menyimpan Hasil Enkripsi

- 3) Selanjutnya adalah menyiapkan kode untuk melakukan dekripsi ketika data tersebut dipanggil kembali untuk ditampilkan pada layar seperti terlihat pada gambar 8.

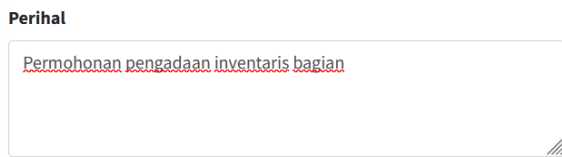
```
<thead>  
<tr>  
<th>Nomor Surat</th>  
<th>Tgl Surat</th>  
<th>Dari</th>  
<th>Perihal</th>  
<th>Ops</th>  
</tr>  
</thead>  
<tbody>  
<tr>  
<td><?php  
$this->encryption->initialize(array('cipher' => 'blowfish'));  
foreach($surat_list as $key){  
$perihal = $this->encryption->decrypt($key->perihal);  
>>  
</td>  
<td><?=$key->no_urut ?><?=$key->kd_surat ?><?=$key->kd_masalah  
<td><?=$key->tanggal ?></td>  
<td><?=$key->dari ?></td>  
<td><?=$perihal ?></td>  
<td><?=$key->ops ?></td>  
</tr>  
</tbody>  
</table>  
<a class="btn btn-sm btn-success" data-toggle="modal" data-target="
```

Gambar 8. Dekripsi Record Tersimpan

E. Hasil Enkripsi dan Dekripsi Menggunakan Algoritma Blowfish

- 1) Hasil enkripsi bagian perihal surat yang tersimpan pada database berdasarkan isian dan kunci enkripsi. Isian

perihal oleh pengguna tersaji pada gambar 9 dan record tersimpan pada database tersaji pada gambar 10.



Gambar 9. Isian Perihal

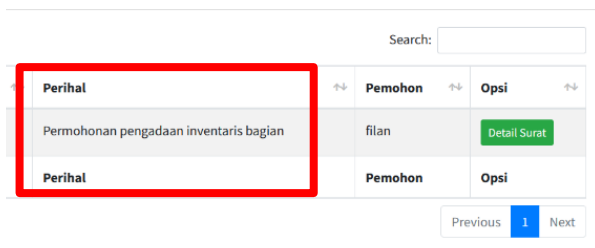


Gambar 10. Record Tersimpan

Dapat dilihat pada gambar 10 bahwa perihal dengan isian “Permohonan pengadaan inventaris bagian” telah terenkripsi menggunakan algoritma blowfish dengan kunci “itpln” sehingga menghasilkan ciphertext seperti yang terlampir pada gambar yaitu :

“9b5541effdfd9938342d16e08233c5b0f1b7ba673ac2ec1ed7be10e0966bdad996a46a9b2e7e464d9dc8eb586e7b0062bf695a6442076078a5b30dc606cabb7fBzeGpsw+p+8P3fE85qtqtsWctiPUUBVWLQcAABQ/9xmOfW78xqBH6u89S7IF5HT2”

2) Hasil dekripsi bagian perihal surat yang ditampilkan ketika dipanggil pada tabel data surat seperti terlihat pada gambar 11.



Gambar 11. Tampilan Dekripsi

Dapat dilihat pada gambar diatas bahwa record berupa ciphertext yang tersimpan pada database telah berhasil didekripsi ketika ditampilkan pada tabel data surat, sehingga output yang dilihat oleh pengguna tetap berupa plaintext.

IV. KESIMPULAN

Penelitian ini menggali berbagai aspek terkait keamanan data surat, optimasi proses manajemen surat, penerapan metodologi pengembangan perangkat lunak RUP, serta kontribusi perangkat lunak terhadap program global dalam mengurangi dampak lingkungan. Peningkatan keamanan data surat dilakukan dengan mengimplementasikan algoritma Blowfish untuk mengenkripsi isi surat sehingga mengurangi

risiko pencurian data saat terjadi peretasan seperti yang dilakukan oleh [2]. Penelitian ini menghasilkan sistem manajemen surat berbasis web yang mengoptimalkan proses di ITPLN, mengurangi hambatan administratif, dan memudahkan penomoran serta pendataan surat meski pegawai tidak berada di kantor. Dengan metodologi RUP yang terstruktur dan berkontribusi terhadap green computing, penelitian ini mendukung sustainable development goals (SDGs) dalam mengurangi dampak lingkungan dari pengembangan perangkat lunak sebagaimana yang dikemukakan oleh [9]. Menggabungkan perkembangan teknologi, optimasi proses, keamanan data, dan kesadaran lingkungan, penelitian ini berkontribusi pada pengembangan sistem informasi yang berkelanjutan dan bertanggung jawab.

REFERENSI

- [1] R. E. G. Rahayu, A. Sutedi, and V. A. Rahayu, “Sistem Informasi Pengelolaan Surat Online Desa Menggunakan Metode Rational Unified Procces Berbasis Web,” *Jurnal Algoritma*, vol. 19, no. 1, pp. 239–246, 2022, doi: <https://doi.org/10.33364/algoritma/v.19-1.1052>.
- [2] E. P. Sitopu, N. Khairina, and R. Muliono, “Sistem Informasi Manajemen Data Surat Dengan Algoritma Blowfish,” *Jurnal Ilmiah Sistem Informasi*, vol. 6, no. 1, pp. 49–59, 2022.
- [3] A. Rahayu, A. P. Ardana, C. Pramudhita, D. Syafitri, and R. Z. Sirega, “Perbandingan Algoritma RSA dengan Algoritma Blowfish Pada Perancangan Aplikasi Keamanan Data,” *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, vol. 7, no. 1, pp. 203–207, 2024.
- [4] M. Dhaini, M. Jaber, A. Fakhereldine, S. Hamdan, and R. A. Haraty, “Green Computing Approaches - A Survey,” *Informatica*, vol. 45, no. 1, pp. 1–12, Mar. 2021, doi: 10.31449/inf.v45i1.2998.
- [5] H. Jatnika, M. F. Rifai, and L. T. E. Napitupulu, “Implementation of the Rational Unified Process (Rup) Method in Designing a Web-Based Certification Scheduling Application (Citation) on Itcc Itpln,” *Syntax Idea*, vol. 5, no. 4, pp. 452–458, Apr. 2023, doi: 10.46799/syntax-idea.v5i4.2188.
- [6] M. Sudarma, S. Ariyani, and P. A. Wicaksana, “Implementation of the Rational Unified Process (RUP) Model in Design Planning of Sales Order Management System,” *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 5, no. 2, pp. 249–265, Aug. 2021, doi: 10.29407/intensif.v5i2.15543.
- [7] Y. Bagus, A. Rahman, and B. Sugiantoro, “The Development of Web-Based Paperless Office System Using CodeIgniter Framework Case Study of Lembaga Pengembangan Cabang Ranting Muhammadiyah,” *Proceeding International Conference on Science and*

- Engineering*, vol. 3, pp. 221–227, Apr. 2020, doi: 10.14421/icse.v3.501.
- [8] S. Soobia.et.al., “Analysis of Software Development Methodologies,” *International Journal of Computing and Digital Systems*, vol. 8, no. 5, pp. 445–460, Jan. 2019, doi: 10.12785/ijcds/080502.
- [9] F. Firmansyah, M. Y. D. Sudirman, and R. I. Putra, “Integrating green computing into rational unified process for sustainable development goals: a comprehensive approach,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 3, pp. 2868–2874, Jun. 2024, doi: 10.11591/ijece.v14i3.pp2868-2874.
- [10] C. R. Suryanto, M. Fajar, and Hasniati, “Pemanfaatan Enkripsi Data Berbasis Algoritma Blowfish Pada Aplikasi Password Manager RememberMe!,” *KHARISMA Tech*, vol. 19, no. 1, pp. 64–74, Nov. 2023, doi: 10.55645/kharismatech.v19i1.421.
- [11] D. Ramalinda, Jayadi, and A. R. Raharja, “Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi,” *Journal of International Multidisciplinary Research*, vol. 2, no. 6, pp. 665–671, Jun. 2024, doi: 10.62504/jimr679.
- [12] R. Silalahi, I. Parlina, Sumarno, I. Gunawan, and W. Saputra, “Implementasi Algoritma Caesar Cipher Dan Algoritma Rsa Untuk Keamanan Data Surat Wasiat Pada Kantor Notaris/PPAT Robert Tampubolon,S.H.,” *Sostech Greenvest*, vol. 1, no. 4, pp. 282–293, Apr. 2021.
- [13] E. Setyawati, C. E. Widjayanti, R. R. Siraiz, and H. Wijoyo, “Pengujian keamanan komputer kriptografi pada surat elektronik berbasis website dengan enkripsi metode MD5,” *Jurnal Manajemen Informatika Jayakarta*, vol. 1, no. 1, p. 56, Feb. 2021, doi: 10.52362/jmijayakarta.v1i1.367.
- [14] T. R. Syafutra, K. Khairil, and E. Suryana, “The Implementation Of Modern Cryptography On Document Data Security,” *Jurnal Media Computer Science*, vol. 1, no. 2, Jul. 2022, doi: 10.37676/jmcs.v1i2.2742.
- [15] H. Nasution, H. Priyanto, and N. Widya, “Penerapan Digital Signature Untuk Persuratan Dengan Menggunakan Metode Algoritma Sha-1 Di Sektor Pertanian, Ketahanan Pangan Dan Perikanan Kab. Mempawah,” *Scientica: Jurnal Ilmiah Sains dan Teknologi*, vol. 2, no. 4, pp. 131–149, 2024.
- [16] A. H. Hasugian, R. A. Putri, and A. S. Zuhri, “Penerapan Metode Elgamal Untuk Mengamankan Teks Pada File Dokumen Word,” *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 4, no. 2, pp. 1143–1153, 2023.
- [17] M. Irvai and N. Efranda, “Implementasi Algoritma SHA512 Pada Keamanan Berita Acara Hasil Sidang Berbasis Web,” *Journal of Information Technology Ampera (JOURNAL-ITA)*, vol. 3, no. 3, pp. 453–466, 2022.