Jurnal Online Universitas Budi Luhur

# SKANIKA

Sistem Komputer dan Teknik Informatika

Vol. 1, No. 1, Mei 2018




UNIVERSITAS BUDI LUHUR

**Diterbitkan oleh:**
Universitas Budi Luhur
Jl. Raya Ciledug Petukangan Utara, Jakarta Selatan

# Editorial Team

**Journal in Chief :**
Dr. Indra, S.Kom, M.T.I, Universitas Budi Luhur, Jakarta, Indonesia
**Google Scholar** | Scopus ID: **57209452300** | SINTA ID: **5978751** | **ORCID**

**Associate (Handling) Editor :**
Samsinar, S.Kom, M.Kom, Universitas Budi Luhur, Jakarta, Indonesia
**Google Scholar** | Scopus ID: **57208868563** | SINTA ID: **6049803** | **ORCID**

**Editorial Board :**
Reva Ragam Santika, S.Kom, M.Kom, Universitas Budi Luhur, Jakarta, Indonesia
**Google Scholar** | Scopus ID: **57226493297** | SINTA ID: **5982758**

Nurwati, S.Kom, M.Kom, Universitas Budi Luhur, Jakarta, Indonesia
**Google Scholar** | Scopus ID: xxxx | SINTA ID: **6068418**

Dani Anggoro, S.Kom., M.Kom., Universitas Muhammadiyah Metro, Jakarta, Indonesia
**Google Scholar** | Scopus ID: xxxx | SINTA ID: **6782419**

Leny Tritanto Ningrum, S.Kom., M.Kom., Universitas Binaniaga Indonesia, Bogor, Indonesia
**Google Scholar** | Scopus ID: xxxx | SINTA ID: **6816386**

Ada Pertanyaan? Chat Via WhatsApp
SKANIKA(6281319)

CERTIFICATE

JOURNAL MENU
Fokus dan Ruang Lingkup
Pernyataan Etika Publikasi
Pernyataan Akses Terbuka
Kebijakan Privasi
Kebijakan Plagiasi
Kebijakan Kearsipan Mandiri
Retraksi dan Koreksi
Pernyataan Hak Cipta & Lisensi
Biaya Publikasi (APC)
Jadwal dan Frekuensi Terbit
Panduan Penulis
Pembatalan Naskah
Proses Peer Review
Pengindeks

INFORMATION
Pembaca
Penulis
Pustakawan

ABOUT AS
Mitra Bestari
Editorial Tim
Sejarah Jurnal
Hubungi Kami

E-ISSN
9 772721 478009
**2721-4788**
**(Berlaku mulai terbitan Vol 3, No.1 Januari 2020)**

JOURNAL TEMPLATE
Article template
Template ini **berlaku mulai Edisi terbitan Januari 2022** Hingga Saat ini yang menggantikan template sebelumnya
Surat Pernyataan Publikasi

INDEXED BY
sinta S3
Google Scholar
GARUDA
ROAD
Crossref
BASE
Dimensions

Kami mengundang para akademisi untuk bergabung dengan tim kami sebagai reviewer di Jurnal SKANIKA dengan mengisi form

(mohon **klik gambar** di bawah ini)

Call For Reviewer 2025

TOOLS PENDUKUNG
MENDELEY
grammarly
turnitin

VISITORS

Visitors
US 94,120 BY 202
SG 11,013 CA 157
ID 2,411 PK 152
CN 452 JP 108
TL 207 RU 101
Pageviews: 185,412
FLAG counter

Jumlah Pengunjung : 00091243

Statistik Pengunjung

JOURNAL CITATION
Scopus -
Citedness
Sinta 3
Sinta Rank
2.54717
Sinta Impact
1216
Citations
Powered by Author Sky DB

MEMBER
RELAWAN JURNAL INDONESIA
ASOSIASI PENGELOLA JURNAL INFORMATIKA DAN KOMPUTER INDONESIA
APJIKOM

forgot password

Kirim email ditujukan ke skanika.fbl@budiluhur.ac.id dengan subject **LostPassword** sertakan username anda pada bagian isi email. Terima kasih.

Maps

**EDITORIAL OFFICE:**

**FAKULTAS TEKNOLOGI INFORMASI - UNIVERSITAS BUDI LUHUR,** Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260. DKI Jakarta, Indonesia. Telp: 021-585 3753 Fax: 021-585 3752

**SKANIKA: Sistem Komputer dan Teknik Informatika** by **FAKULTAS TEKNOLOGI INFORMASI - UNIVERSITAS BUDI LUHUR**

is licensed under **CC BY-SA 4.0**

View Jurnal SKANIKA Stats 00091243

Platform & workflow by OJS / PKP

# Reviewer

**Mitra Bestari**

**Universitas Budi Luhur, Jakarta, Indonesia**
Dr. Arief Wibowo, S.Kom., M.Kom. **Google Scholar** | Scopus ID: **57195675462** | SINTA ID: **259862** | **ORCID**
Dr. Achmad Solichin, S.Kom., M.T.I. **Google Scholar** | Scopus ID: **57193909834** | SINTA ID: **259856** | **ORCID**
Dr. Mohammad Syafrullah, M.Kom., M.Sc. **Google Scholar** | Scopus ID: **57201861985** | SINTA ID: **5984532** | **ORCID**
Dr. Utomo Budiyanto, M.Kom., M.Sc. **Google Scholar** | Scopus ID: **57198358682** | SINTA ID: **6695162**
Dr. Imelda, S.Kom., M.Kom. **Google Scholar** | Scopus ID: **57198358682** | SINTA ID: **6662371**
Hilman Akhyar Damanik, S.Kom., M.Kom. **Google Scholar** | Scopus ID: **57209022275** | SINTA ID: **6694077**

**UPN Veteran Yogyakarta, Indonesia**
Dr. Heriyanto, A.Md, S.Kom., M.Cs. **Google Scholar** | Scopus ID: **57223026215** | SINTA ID: **6200173** | **ORCID**

**STMIK STIKOM Indonesia, Bali, Indonesia**
Dr. Ir. Putu Sugiartawan, M.Agb., M.Cs. **Google Scholar** | Scopus ID: **57210473976** | SINTA ID: **6001478**

**STMIK PPKIA Pradnya Paramita, Malang, Indonesia**
Dr. Khoerul Anwar, ST., MT. **Google Scholar** | Scopus ID: **57199358561** | SINTA ID: **6022960** | **ORCID**

**Institut AIN Syekh Nurjati Cirebon, Cirebon, Indonesia**
Dr. Darwan, M.Kom. **Google Scholar** | Scopus ID: **57255757000** | SINTA ID: **6587370** | **ORCID**

**International Islamic University Malaysia, Kuala Lumpur, Malaysia**
Dwi Pebrianti, Ph.D. **Google Scholar** | Scopus ID: **55268466200** | SINTA ID: **6039003** | **ORCID**

**Universitas Bumigora, Mataram, NTB, Indonesia**
Dr. Helna Wardhana, M.Kom. **Google Scholar** | Scopus ID: **57205488284** | SINTA ID: **6070603**

**Universitas Mercu Buana, Yogyakarta, Indonesia**
Arita Witanti, S.T., M.T. **Google Scholar** | Scopus ID: **59251143200** | SINTA ID: **5973841**

**Universitas AKPRIND, Yogyakarta, Indonesia**
Dr. Suwarto Raharjo, S.Si., M.Kom. **Google Scholar** | Scopus ID: **56192446500** | SINTA ID: **152252** | **ORCID**

**Universitas Nusa Cendana, NTT, Indonesia**
Dr. Yulianto Triwahyuadi Polly, S.Kom., M.Cs. **Google Scholar** | Scopus ID: **57348238100** | SINTA ID: **6024274** | **ORCID**

**Universitas Mulawarman, Samarinda, Indonesia**
Prof. Dr. Arinditia Septiarini, S.T., M.Cs **Google Scholar** | Scopus ID: **56530676100** | SINTA ID: **258119** | **ORCID**

**Universitas Gadjah Mada, Samarinda, Indonesia**
Dr. Dyah Aruming Tyas. **Google Scholar** | Scopus ID: **57201703672** | SINTA ID: **6773420** | **ORCID**

**Universitas Esa Unggul, Jakarta, Indonesia**
Ir. Sawali Wahyu, S.Kom., M.Kom. **Google Scholar** | Scopus ID: **57710550400** | SINTA ID: **6744040** | **ORCID**

**Politeknik Kota Malang, Indonesia**
Mohammad Faried Rahmat,. S.ST., M.Tr.T **Google Scholar** | Scopus ID: **60072102800** | SINTA ID: **6851472** | **ORCID**

**Universitas Dharma AUB Surakarta, Indonesia**
Izzan Julda D.E Purwadi Putra S.T., M.Kom. **Google Scholar** | Scopus ID: **58419142800** | SINTA ID: **6985656** | **ORCID**

**Universitas Ma Chung, Malang, Indonesia**
Windra Swastika, Ph.D. **Google Scholar** | Scopus ID: **55773044200** | SINTA ID: **257757** | **ORCID**

Ada Pertanyaan? Chat Via WhatsApp
SKANIKA@UBL.AC.ID

CERTIFICATE





E-ISSN
9 772721 478009
**2721-4788**
**(Berlaku mulai terbitan Vol 3, No.1 Januari 2020)**

JOURNAL TEMPLATE

Article template

Template ini **berlaku mulai Edisi terbitan Januari 2022** Hingga Saat ini yang menggunakan template sebelumnya

Surat Pernyataan Publikasi

INDEXED BY

Kami mengundang para akademisi untuk bergabung dengan tim kami sebagai reviewer di Jurnal SKANIKA dengan mengisi form

(mohon **klik gambar** di bawah ini)

Call For Reviewer 2025

TOOLS PENDUKUNG

VISITORS




Jumlah Pengunjung : **00091244**

Statistik Pengunjung

JOURNAL CITATION

Scopus - Citedness
Sinta 3 Sinta Rank
2.54717 Sinta Impact
1216 Citations
Powered by Author Sky DB

MEMBER

Kirim email ditujukan ke skanika.fbl@budiluhur.ac.id dengan subject **LostPassword** sertakan username anda pada bagian isi email. Terima kasih.

Maps

**EDITORIAL OFFICE:**

**FAKULTAS TEKNOLOGI INFORMASI - UNIVERSITAS BUDI LUHUR,** Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260. DKI Jakarta, Indonesia. Telp: 021-585 3753 Fax: 021-585 3752

**SKANIKA: Sistem Komputer dan Teknik Informatika** by **FAKULTAS TEKNOLOGI INFORMASI - UNIVERSITAS BUDI LUHUR**

is licensed under **CC BY-SA 4.0**

View Jurnal SKANIKA Stats **00091244**

Platform & workflow by OJS / PKP

# Vol. 1 No. 2 (2018): Jurnal SKANIKA Mei 2018



SKANIKA: Sistem Komputer dan Teknik Informatika adalah Jurnal ilmiah diterbitkan secara berkala di Fakultas Teknologi Informasi Universitas Budi Luhur mulai Maret tahun 2018. Jurnal ini bertujuan menyebarluaskan hasil penelitian di bidang Sistem Komputer dan Teknik Informatika. Jurnal SKANIKA mulai tahun 2021 terbit sebanyak 2 (dua) kali dalam setahun yaitu pada bulan Januari dan Juli. Pemuatan artikel dan pemesanan jurnal dialamatkan ke kantor redaksi.

**Published:** 2018-05-31

## Articles


**MONITORING SISTEM PENYIRAM TANAMAN OTOMATIS DALAM RUMAH KACA BERBASIS ARDUINO UNO R3**
Rifki Fuad, I Wayan Degeng 540-544
download PDF Artikel Dibaca: 1323 kali. Artikel Diunduh: 2472 kali.

**IMPLEMENTASI LOCATION BASED SERVICE DAN ALGORITMA POLYLINE PADA APLIKASI PEMESANAN MOBIL DI UNIVERSITAS BUDI LUHUR BERBASIS ANDROID**
Yusup Supriyadi, Painem Painem 751-757
download PDF Artikel Dibaca: 1079 kali. Artikel Diunduh: 876 kali.

**IMPLEMENTASI PENGAMANAN EMAIL MENGGUNAKAN METODE BLOWFISH BERBASIS WEB PADA UPT PUSKESMAS PONDOK KACANG TIMUR**
Erick Erwin Nylis , Purwanto Purwanto 570-576
download PDF Artikel Dibaca: 951 kali. Artikel Diunduh: 692 kali.

**IMPLEMENTASI KRIPTOGRAFI PADA PENGIRIMAN PESAN EMAIL DENGAN MENGGUNAKAN METODE RC4 DAN BLOWFISH BERBASIS WEB PADA PT.DASCOM JAYA SAKTI**
Frengki Danil Zain Rohman , Mufti Mufti 788-793
download pdf Artikel Dibaca: 1402 kali. Artikel Diunduh: 1236 kali.

**ALGORITMA ENKRIPSI RC4 (RIVEST CODE 4) PADA APLIKASI CATATAN TEKS ANDROID PADA PT INTERNUSA FOOD**
Berliana Putri Natalia , Ferdiansyah Ferdiansyah 604-610
download PDF Artikel Dibaca: 1727 kali. Artikel Diunduh: 573 kali.

**SISTEM KEAMANAN DATABASE MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD(AES-128) STUDI KASUS : RED AVENUE INDONESIA**
Faris Akbar, Sejati Waluyo 821-828
download pdf Artikel Dibaca: 1880 kali. Artikel Diunduh: 2380 kali.

**PENERAPAN KOMPRESI CITRA DIGITAL DENGAN METODE KUANTISASI WARNA MENGGUNAKAN ALGORITMA K-MEANS PADA WEBSITE PEDULI SEKITAR**
Sara Famayla, Muhammad Ainur Rony 431-438
Download PDF Artikel Dibaca: 1581 kali. Artikel Diunduh: 1127 kali.

**SISTEM SWITCHING ENERGI LISTRIK TURBIN ANGIN DAN PLN BERBASIS ARDUINO**
Farhan Farhan, Irawan Irawan 635-641
download PDF Artikel Dibaca: 1256 kali. Artikel Diunduh: 1938 kali.

**DETEKSI, PELACAKAN DAN JUMLAH KENDARAAN DENGAN MOVING AVERAGE SUBTRACTION DAN HUNGARIAN**
Amran Swandy Simamora , Imelda Imelda 855-861
download pdf Artikel Dibaca: 1664 kali. Artikel Diunduh: 916 kali.

**PENGAMANAN DATA PADA APLIKASI ANDROID DENGAN ALGORITMA BLOWFISH DAN AES-128 (STUDI KASUS PADA FITUR BLUCAREER APLIKASI BLUCAMPUS UNIVERSITAS BUDI LUHUR)**
Khaeri Diniari, Achmad Solichin 469-474
download PDF Artikel Dibaca: 910 kali. Artikel Diunduh: 872 kali.

**APLIKASI ENKRIPSI DATA PENILAIAN SISWA PADA DATABASE MENGGUNAKAN ALGORITMA KRIPTOGRAFI (AES-128) BERBASIS WEB**
Faldi Rachmat Nopianto , Ferdiansyah Ferdiansyah 669-675
download PDF Artikel Dibaca: 1329 kali. Artikel Diunduh: 1144 kali.

**APLIKASI MENGAMANKAN EMAIL DENGAN MENGGUNAKAN METODE ALGORITMA KRIPTOGRAFI RC6 PADA PERCETAKAN LIBRADO**
Seh Anang Maulana , Titin Fatimah 498-502
download PDF Artikel Dibaca: 1199 kali. Artikel Diunduh: 821 kali.

**APLIKASI EMAIL (ELECTRONIC MAIL) MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-128) DAN ALGORITMA RIVEST CIPHER 4 (RC4) BERBASIS WEB**
Ryfan Aditya Indra , Wahyu Pramusinto 704-710
download PDF Artikel Dibaca: 1051 kali. Artikel Diunduh: 1049 kali.

**APLIKASI KEAMANAN EMAIL DENGAN METODE RC4 (RIVEST CODE 4) DAN DES (DATA ENCRYPTION STANDARD) BERBASIS MOBILE ANDROID PADA PT. TIRTA ABADI GEMILANG**
Diki Firmansyah, Rizky Tahara Shita 528-533
download PDF Artikel Dibaca: 1490 kali. Artikel Diunduh: 781 kali.

**IMPLEMENTASI ALGORITMA APRIORI UNTUK MEMPREDIKSI PENJUALAN TIKET BERBASIS DEKSTOP PADA PT. NADIA TRAVEL**
Thisa Tri Utami , Mohammad Syafrullah 739-744
download PDF Artikel Dibaca: 1518 kali. Artikel Diunduh: 1312 kali.

**APLIKASI PENGAMANAN SMS (SHORT MESSAGE SERVICE) DENGAN MENGGUNAKAN ALGORITMA AES-128 BERBASIS ANDROID PADA KANTOR NOTARIS RINA ADRIANI S.H**
Anita Fauziah, Dewi Kusumaningsih 558-564
download PDF Artikel Dibaca: 1499 kali. Artikel Diunduh: 702 kali.

**APLIKASI KRIPTOGRAFI PENGAMANAN DATABASE MENGGUNAKAN METODE AES DAN VIGENERE BERBASIS DESKTOP PADA PADA DIVISI PENCEGAHAN DAN PENANGGULANGAN HIV AIDS YAYASAN KAPETA**
Denny Eka Erlianto , Painem Painem 773-779
download pdf Artikel Dibaca: 1600 kali. Artikel Diunduh: 746 kali.

**APLIKASI PENCARIAN INFORMASI KONTEN MENGGUNAKAN ALGORITMA KNUTH MORRIS PRATT PADA APLIKASI LIBRO PUSTAKA DIGITAL**
Rifky Praptama, Ferdiansyah Ferdiansyah 591-596
download PDF Artikel Dibaca: 1658 kali. Artikel Diunduh: 827 kali.

**IMPLEMENTASI ALGORITMA MULTIFACTOR EVALUATION PROCESS (MFEP) UNTUK SELEKSI PENERIMAAN CALON KARYAWAN**
Rian Nurjaman, Ir. Siswanto 807-814
download pdf Artikel Dibaca: 1093 kali. Artikel Diunduh: 1280 kali.

**IMPLEMENTASI ALGORITMA ENKRIPSI CAESAR CIPHER DAN VIGENERE CIPHER PADA APLIKASI MOBILE DAN REST API DATA PERUSAHAAN PADA PT. CENTRAL CAPITAL FUTURES**
Bagas Wahyu Utomo , Subandi Subandi 624-629
download PDF Artikel Dibaca: 1495 kali. Artikel Diunduh: 949 kali.

**APLIKASI PENILAIAN KINERJA GURU MENGGUNAKAN METODE SIMPLE ADDITIVE WEIGHTING BERBASIS WEB**
Agung Gumelar, Alexander J.P Sibarani 842-848
download pdf Artikel Dibaca: 1167 kali. Artikel Diunduh: 787 kali.

**OPTIMASI WEB SERVICE DENGAN PENERAPAN ALGORITMA KOMPRESI LZW: STUDI KASUS APLIKASI BLUCAMPUS UNIVERSITAS BUDI LUHUR**
Mochammad Andika Putra , Achmad Solichin 455-462
download PDF Artikel Dibaca: 1129 kali. Artikel Diunduh: 860 kali.

**APLIKASI CHATTING NOTARIS BERBASIS ANDROID DENGAN METODE KRIPTOGRAFI AES-128 DAN BLOWFISH**
Zaid Fadhlurrahman, Pipin Farida Ariyani 656-661
download PDF Artikel Dibaca: 1051 kali. Artikel Diunduh: 1312 kali.

**IMPLEMENTASI ALGORITMA HASH SHA-1 DISERTAI TEKNIK KRIPTOGRAFI METODE AFFINE CIPHER DAN AES-256 PADA APLIKASI CHATTING BERBASIS ANDROID**
Deditian Nurhadid, Noni Juliasari 486-490
download PDF Artikel Dibaca: 1575 kali. Artikel Diunduh: 863 kali.

**PENINGKATAN KEAMANAN LOGIN WEBSITE DENGAN IMPLEMENTASI ONE TIME PASSWORD MENGGUNAKAN ALGORITMA SHA1 DAN MD5 BERBASIS MOBILE**
Muhammad Sonny Ramadhan , Pipin Farida Ariyani 689-696
download PDF Artikel Dibaca: 2738 kali. Artikel Diunduh: 1386 kali.

**ALGORITMA KOMPRESI LZ77 DAN HUFFMAN UNTUK MEDIA SOSIAL BERBASIS ANDROID STUDI DI UNIVERSITAS BUDI LUHUR**
Fransisco Fransisco, Rizky Tahara Shita 514-521
download PDF Artikel Dibaca: 1197 kali. Artikel Diunduh: 1235 kali.

**APLIKASI PENGAMANAN SURAT ELEKTRONIK (EMAIL) MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD 128 (AES-128) DAN RIVEST CIPHER CODE 4 (RC4) BERBASIS WEB**
Rauf Riyantono, Wahyu Pramusinto 725-731
download PDF Artikel Dibaca: 1337 kali. Artikel Diunduh: 1238 kali.

**IMPLEMENTASI ALGORITMA BLOWFISH DAN ALGORITMA RC4 PADA APLIKASI KEAMANAN EMAIL**
Hatanu Prasidya Martosedono , Purwanto Purwanto 545-550
download PDF Artikel Dibaca: 1425 kali. Artikel Diunduh: 1102 kali.

**IMPLEMENTASI KRIPTOGRAFI UNTUK PENGAMANAN PESAN TEKS PADA APLIKASI CHATTING BERBASIS ANDROID DENGAN METODE VIGENERE CIPHER PADA SMK NEGERI 7 KOTA TANGERANG**
Rudiyanto Rudiyanto, Safrina Amini 758-765
download pdf Artikel Dibaca: 1186 kali. Artikel Diunduh: 1420 kali.

**APLIKASI PENDETEKSI ELEMEN PANAS API UNTUK PENCEGAHAN BENCANA KEBAKARAN BERBASIS WEB DENGAN RAPBERRY PI, FLAME SENSOR DAN NOTIFIKASI TELEGRAM PADA SUKU DINAS PENANGGULANGAN KEBAKARAN DAN PENYELAMATAN DKI JAKARTA**
Panroy Vallientinus, Ferdiansyah Ferdiansyah 577-582
download PDF Artikel Dibaca: 2006 kali. Artikel Diunduh: 835 kali.

**IMPLEMENTASI METODE WEIGHTED PRODUCT UNTUK EMILIHAN SISWA-SISWI UNGGULAN BERBASIS WEB PADA SMA NEGERI 5 TANGERANG SELATAN**
Eko Saputro, Haris Munandar 794-800
download pdf Artikel Dibaca: 1349 kali. Artikel Diunduh: 660 kali.

**APLIKASI SISTEM PENUNJANG KEPUTUSAN PEMILIHAN KARYAWAN TERBAIK PADA PT. MITRA SINERGI ADHITAMA DENGAN METODE SIMPLE ADDITIVE WEIGHTING (SAW) BERBASIS DESKTOP**
Danang Zakaria, Sri Mulyati 611-617
download PDF Artikel Dibaca: 1069 kali. Artikel Diunduh: 1037 kali.

**APLIKASI PREDIKSI KELULUSAN UJIAN NASIONAL MENGGUNAKAN ALGORITMA K-NEAREST NEIGHBOR DENGAN PENGUKURAN JARAK MANHATTAN DISTANCE**
Ary Maulana Malik , Alexander J.P. Sibarani 829-835
download pdf Artikel Dibaca: 1063 kali. Artikel Diunduh: 954 kali.

**PENCARIAN RUTE TERPENDEK MENUJU LOKASI LEMBAGA SOSIAL MENGGUNAKAN ALGORITMA DIJKSTRA BERBASIS ANDROID PADA APLIKASI PEDULI SEKITAR**
Agus Santoso, Muhammad Ainur Rony 439-447
Download PDF Artikel Dibaca: 1444 kali. Artikel Diunduh: 0 kali.

**APLIKASI KENDALI CATUDAYA MODEM MENGGUNAKAN ARDUINO ETHERNET, SENSOR SUHU DAN ARUS LISTRIK BERBASIS JAVA PADA NODE SENTRAL PT. APLIKANUSA LINTASARTA**
Asif Raswono, Subandi Subandi 642-649
download PDF Artikel Dibaca: 912 kali. Artikel Diunduh: 697 kali.

**IMPLEMENTASI METODE SIMPLE ADDITIVE WEIGHTING UNTUK MEMBERI REKOMENDASI OBAT DIABETES UNTUK PASIEN BERBASIS JAVA DESKTOP**
Ahmad Fitrah Maulana , Hari Soetanto 862-868
download pdf Artikel Dibaca: 1410 kali. Artikel Diunduh: 795 kali.

**IMPLEMENTASI ONE TIME PASSWORD DENGAN ALGORITMA HASH SHA-512 BERBASIS WEB UNTUK KEAMANAN DATA SISWA**
Muhamad Nur Faizal Afrianto , Siswanto Siswanto 475-480
download PDF Artikel Dibaca: 1847 kali. Artikel Diunduh: 1730 kali.

**APLIKASI PENGAMANAN CHAT DENGAN ALGORITMA CAST-128 BERBASIS WEB PADA PT. TJOKRO BERSAUDARA**
Akhmad Affandi, Siswanto Siswanto 676-683
download PDF Artikel Dibaca: 1917 kali. Artikel Diunduh: 880 kali.

**IMPLEMENTASI STEGANOGRAFI DENGAN METODE END OF FILE PADA MEDIA AUDIO DAN KRIPTOGRAFI METODE RSA SERTA VIGENERE CIPHER BERBASIS JAVA DESKTOP UNTUK MENGAMANKAN DATA**
Muhammad Agung A. Djafar , Noni Juliasari 503-507
download PDF Artikel Dibaca: 1075 kali. Artikel Diunduh: 837 kali.

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI DENGAN ALGORITMA CAESAR CIPHER, ADVANCED ENCRYPTION STANDARD 256, DAN RC6 UNTUK APLIKASI CHATTING BERBASIS ANDROID**
Dimas Bayu Gumelar , Wahyu Pramusinto 711-717
download PDF Artikel Dibaca: 1784 kali. Artikel Diunduh: 1205 kali.

**APLIKASI PENGAMANAN EMAIL BERBASIS ANDROID DENGAN ALGORITMA KRIPTOGRAFI AES-128DAN RC4 PADAPT TIRTA INVESTAMA**
Andrian Lesmana, Rizky Tahara Shita 534-539
download PDF Artikel Dibaca: 1017 kali. Artikel Diunduh: 759 kali.

**PENGIMPLEMENTASIAN ONE TIME PASSWORD DAN NOTIFIKASI EMAIL MENGGUNAKAN FUNGSI HASH SHA-512 BERBASIS WEB PADA SMK CYBER MEDIA**
Nanda Imani Yahya , Safrina Amini 745-750
download PDF Artikel Dibaca: 1386 kali. Artikel Diunduh: 1466 kali.

**IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD-128 (AES-128) UNTUK PENGAMANAN DATABASE BERBASIS DESKTOP PADA ICALTOYS**
Tritera Erlangga, Dewi Kusumaningsih 565-569
download PDF Artikel Dibaca: 1399 kali. Artikel Diunduh: 938 kali.

**ALGORITMA RSA UNTUK PENGAMANAN DATA LOKASI PADA API BERBASIS RESTFUL WEB SERVICE**
Akbar Maulana Putra , Painem Painem 780-787
download pdf Artikel Dibaca: 1394 kali. Artikel Diunduh: 885 kali.

**APLIKASI KEAMANAN DATABASE MENGGUNAKAN ALGORITMA KRIPTOGRAFI TRIANGLE CHAIN CIPHER BERBASIS DESKTOP**
Ajat Sudrajat, Windarto Windarto 597-603
download PDF Artikel Dibaca: 1194 kali. Artikel Diunduh: 1577 kali.

**APLIKASI KRIPTOGRAFI UNTUK KEAMANAN DATABSE DENGAN METODE RC4 DAN ELGAMAL BERBASIS WEB PADA JXL DESIGN CO**
Gilang Ammary, Sri Mulyati 815-820
download pdf Artikel Dibaca: 1548 kali. Artikel Diunduh: 1057 kali.

**SISTEM PENGENDALI TEMPERATUR PADA PANEL SURYA MENGGUNAKAN MEDIA PENYEMPROTAN AIR OTOMATIS BERBASIS ARDUINO**
Qory Hadromi, Yani Prabowo 630-634
download PDF Artikel Dibaca: 1227 kali. Artikel Diunduh: 1262 kali.

**SISTEM KONTROL DAN MONITORING MENGGUNAKAN ARDUINO**
Diana Juwi Megatarini , Yan Everhard 849-854
download pdf Artikel Dibaca: 1538 kali. Artikel Diunduh: 1688 kali.

**PROTOTIPE SISTEM PENDUKUNG KEPUTUSAN UNTUK PENENTUAN GURU TELADAN PADA SMK ERA INFORMATIKA**
Suherman Achmad, Achmad Solichin 463-468
download PDF Artikel Dibaca: 1386 kali. Artikel Diunduh: 902 kali.

**IMPLEMENTASI KRIPTOGRAFI EMAIL BERBASIS ANDROID DENGAN METODE ELGAMAL PADA PT SUDATA MAKMUR**
Jaqfar Sholeh, Ferdiansyah Ferdiansyah 662-668
download PDF Artikel Dibaca: 1203 kali. Artikel Diunduh: 636 kali.

**APLIKASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA RC4 DAN DES UNTUK MENGAMANKAN PESAN EMAIL**
Aldi Yuliansyah, Noni Juliasari 491-497
download PDF Artikel Dibaca: 1327 kali. Artikel Diunduh: 866 kali.

**ANALISIS SENTIMEN PENGGUNA TWITTER TERHADAP PARTAI POLITIK PENDUKUNG CALON GUBERNUR DI JAKARTA MENGGUNAKAN ALGORITMA C4.5 DECISION TREE LEARNING**
Muhammad Rizqo Fajriansyah , Siswanto Siswanto 697-703
download PDF Artikel Dibaca: 2041 kali. Artikel Diunduh: 1669 kali.

**ALGORITMA DIJKSTRA DALAM MENENTUKAN JARAK TERDEKAT PENCARIAN MINIMAL STORE**
Ricky Anwar Tirta , Rizky Tahara Shita 522-527
download PDF Artikel Dibaca: 1545 kali. Artikel Diunduh: 819 kali.

**KEAMANAN ALGORITMA KRIPTOGRAFI DATABASE MENGGUNAKAN METODE ADVANCED ENCRYPTION STANDARD (AES-128) BERBASIS DESKTOP**
Pandu Pradinata, Muhammad Syafrullah 732-738
download PDF Artikel Dibaca: 1372 kali. Artikel Diunduh: 971 kali.

**APLIKASI STEGANOGRAFI DENGAN METODE TRACK FREE ATOM DAN KRIPTOGRAFI MENGGUNAKAN METODE AES-128 UNTUK PENGAMANAN PESAN PADA FILE MP4 BERBASIS ANDROID**
Hidayatul Ichwan, Dewi Kusumaningsih 551-557
download PDF Artikel Dibaca: 1092 kali. Artikel Diunduh: 676 kali.

**IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN METODE BLOWFISH DAN BASE64 UNTUK MENGAMANKAN EMAIL BERBASIS WEB**
Rizki Ripai, Safrina Amini 766-772
download pdf Artikel Dibaca: 1635 kali. Artikel Diunduh: 1048 kali.

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI VIGENER CIPHER DAN AFFINE CIPHER UNTUK MENGAMANKAN PESAN PADA APLIKASI CHATTING BERBASIS ANDROID**
Muhammad Ricky Darmawan , Windarto Windarto 583-590
download PDF Artikel Dibaca: 1100 kali. Artikel Diunduh: 920 kali.

**IMPLEMENTASI KEAMANAN DATABASE MENGGUNAKAN ALGORITMA VIGENERE CIPHER DAN RIVEST SHAMIR ADLEMAN (RSA) BERBASIS DESKTOP**
Ahsanul Rahman, Sri Mulyati 801-806
download pdf Artikel Dibaca: 1381 kali. Artikel Diunduh: 968 kali.

**APLIKASI MOBILE ONE TIME PASSWORD MENGGUNAKAN ALGORITMA MD5 DAN SHA1 UNTUK MENINGKATKAN KEAMANAN WEBSITE**
Gafi Husni Editya , Sri Mulyati 618-623
download PDF Artikel Dibaca: 1658 kali. Artikel Diunduh: 1646 kali.

**PENERAPAN ALGORITMA MINIMAX DALAM PERMAINAN DAKON PADA SD NEGERI 04 PONDOK RANJI**
Trisna Ayu Suryatin Dwi Putri, Joko Christian Chandra 836-841
download pdf Artikel Dibaca: 1630 kali. Artikel Diunduh: 1585 kali.

**IMPLEMENTASI ONE TIME PASSWORD PADA SISTEM LOGIN DENGAN ALGORITMA SHA-256 DAN DES PADA APLIKASI EO BLUCAMPUS BERBASIS CLIENT SERVER**
Anggit Prayogo, Muhammad Ainur Rony 448-454
download PDF Artikel Dibaca: 1704 kali. Artikel Diunduh: 2508 kali.

**PEMBERI NUTRISI CAIRAN OTOMATIS UNTUK TANAMAN BERBASIS ARDUINO UNO DENGAN MENGGUNAKAN WEB**
Muhammad Eko Yunanto , Irawan Irawan 650-655
download PDF Artikel Dibaca: 1128 kali. Artikel Diunduh: 1360 kali.

**APLIKASI PRESENSI SISWA PADA PT. SAMUDERA ANUGERAH MENGGUNAKAN METODE GEOFENCING DAN PERHITUNGAN JARAK MENGGUNAKAN ALGORITMA EUCLIDEAN DISTANCE BERBASIS ANDROID**
Anissa Shinta Ahmasetyosari , Titin Fatimah 481-485
download PDF Artikel Dibaca: 2173 kali. Artikel Diunduh: 1729 kali.

**SISTEM PENGAMANAN GAMBAR MENGGUNAKAN ALGORITMA AES 256 BERBASISJAVA MOBILE PADA PT.ANTAR MITRA SEMBADA**
Bintang Kristoper Simanjuntak , Siswanto Siswanto 684-688
download PDF Artikel Dibaca: 1621 kali. Artikel Diunduh: 828 kali.

**KEAMANAN DATABASE DENGAN METODE RIVEST CODE 4 (RC4) DAN CAESAR CIPHER BERBASIS DESKTOP**
Achmad Sri Muharyanto , Titin Fatimah 508-513
download PDF Artikel Dibaca: 1242 kali. Artikel Diunduh: 1260 kali.

**APLIKASI PEMBERI PAKAN IKAN OTOMATIS MENGGUNAKAN MIKROKONTROLER ESP8266 BERBASIS WEB (STUDI KASUS : GEDUNG GRAHA MITRA)**
Ridho Saputra, M. Syafrullah 718-724
download PDF Artikel Dibaca: 1680 kali. Artikel Diunduh: 1567 kali.


Ada Pertanyaan? Chat Via WhatsApp silakan klik logo WA

CERTIFICATE

JOURNAL MENU
Fokus dan Ruang Lingkup
Pernyataan Etika Publikasi
Pernyataan Akses Terbuka
Kebijakan Privasi
Kebijakan Plagiasi
Kebijakan Kearsipan Mandiri
Retraksi dan Koreksi
Pernyataan Hak Cipta & Lisensi
Biaya Publikasi (APC)
Jadwal dan Frekuensi Terbit
Panduan Penulis
Pembatalan Naskah
Proses Peer Review
Pengindeks

INFORMATION
Pembaca
Penulis
Pustakawan

ABOUT AS
Mitra Bestari
Editorial Tim
Sejarah Jurnal
Hubungi Kami

E-ISSN
2721-4788
(Berlaku mulai terbitan Vol 3, No.1 Januari 2020)

JOURNAL TEMPLATE
Article template
Template ini **berlaku mulai Edisi terbitan Januari 2022** Hingga Saat ini yang menggantikan template sebelumnya
Surat Pernyataan Publikasi

INDEXED BY

Kami mengundang para akademisi untuk bergabung dengan tim kami sebagai reviewer di Jurnal SKANIKA dengan mengisi form

(mohon **klik gambar** di bawah ini)

Call For Reviewer 2025

TOOLS PENDUKUNG

VISITORS

Jumlah Pengunjung :

Statistik Pengunjung

JOURNAL CITATION
Scopus - Citedness
Sinta 3 Sinta Rank
2.54717 Sinta Impact
1216 Citations

MEMBER

Kirim email ditujukan ke skanika.fti@budiluhur.ac.id dengan subject **LostPassword** sertakan username anda pada bagian isi email. Terima kasih.

**EDITORIAL OFFICE:**

**FAKULTAS TEKNOLOGI INFORMASI - UNIVERSITAS BUDI LUHUR,** Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260. DKI Jakarta, Indonesia. Telp: 021-585 3753 Fax: 021-585 3752

SKANIKA: Sistem Komputer dan Teknik Informatika by FAKULTAS TEKNOLOGI INFORMASI - UNIVERSITAS BUDI LUHUR is licensed under CC BY-SA 4.0

View Jurnal SKANIKA Stats

Platform & workflow by OJS / PKP

# PENINGKATAN KEAMANAN *LOGIN* WEBSITE DENGAN IMPLEMENTASI ONE TIME *PASSWORD* MENGGUNAKAN ALGORITMA SHA1 DAN MD5 BERBASIS MOBILE

**Muhammad Sonny Ramadhan**[1)], **Pipin Farida Ariyani**[2)]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan 12260
Tlp. 021-5853753, Fax. 021-5866369
Email : ramadhansonny@gmail.com[1)], pipin.faridaariyani@budiluhur.ac.id[2)]

***Abstrak***

*CV. Bintang Kharisma adalah perusahaan penyedia alat berat yang biasa bekerjasama dengan perusahaan-perusahaan yang bergerak di bidang pembangunan infrastruktur. Perusahaan ini menyimpan data penting seluruh pelanggan dan perusahaan yang tidak boleh diketahui oleh sembarang pihak. Sistem informasi berbasis online dapat digunakan untuk menunjang kegiatan di dalam suatu perusahaan. Sistem menjadi sangat rentan apabila dapat di akses oleh orang yang tidak berkepentingan sehingga dibutuhkan sistem login. Pada umumnya seseorang akan menggunakan password yang mudah diingat dan ditebak oleh orang lain atau menggunakan password yang tidak pernah berubah. Disisi lain password dapat dengan mudah diketahui oleh pihak lain dengan cara sniffing atau penyadapan. Hal tersebut membuat password tidak aman digunakan untuk mengakses sistem informasi. Maka dari itu, agar dapat mencegah terjadinya penyusupan kedalam sistem informasi dibuat sistem otentikasi berupa kode unik sekali pakai yang disebut One Time Password. Karena penggunaan smartphone android yang saat ini semakin marak digunakan.maka penelitian ini melakukan pemanfaatan smartphone android sebagai pengganti token untuk mengimplementasikan one time password. Untuk membangkitkan one time password digunakan algoritma Message Digest 5 (MD5) dan Secure Hash Algorithm 1 (SHA1) dan sedikit penambahan algoritma Time-Based One Time Password (TOTP) yang membangkitkan enam digit bilangan yang akan berubah setiap 60 detik. Penelitian ini mampu memberikan keamanan pada saat mengakses login pada sistem informasi karena kode yang dihasilkan dari one time password ini selalu berubah dan tidak dapat digunakan kembali untuk mengakses sistem sehingga sistem tidak dapat dengan mudah dibobol oleh orang lain.*

**Kata kunci** : *One Time Password,* Android, MD5, SHA1

## 1. PENDAHULUAN

Teknologi saat ini telah berkembang dengan sangat pesat, tentunya tingkat keamanan yang tinggi juga semakin diperlukan bersamaan dengan majunya teknologi. Sistem *login* merupakan suatu hal yang pasti ditemukan dan merupakan salah satu aspek penting di dalam dunia *internet,* yang perlu diperhatikan keamanannya. *Internet* dibangun melalui jaringan komputer yang saling terhubung, dengan begitu banyaknya *user* yang terhubung dalam jaringan, suatu data maupun informasi menjadi sangat rentan terhadap serangan dari pihak-pihak luar yang tidak berwenang.

Hal ini membuat seluruh data dan informasi dapat dengan mudah diakses oleh siapapun. Tidak hanya bisa diakses oleh orang yang berwenang atau berkepentingan, tetapi juga oleh orang lain yang ingin menggunakannya untuk kepentingan pribadi dengan cara mencuri data dan informasi dari sistem komputer tersebut (peretas). Untuk itu sistem dituntut agar dapat mengetahui pengguna atau *user*yang akan menggunakan sistem adalah pihak yang telah diberi izin atau yang berkepentingan. Pengguna haruslah mengidentifikasi dirinya ke sistem, dan sistem harus memastikan apakah identifikasi tersebut otentik atau tidak.

CV. Bintang Kharisma adalah perusahaan jasa penyedia alat berat yang biasa bekerjasama dengan perusahaan-perusahaan yang bergerak di bidang pembangunan infrastruktur. Perusahaan ini juga menyimpan data penting seluruh pelanggan dan perusahaan yang tidak boleh diketahui oleh sembarang orang supaya tidak terjadi hal-hal merugikan yang tidak diinginkan.

Selama ini *website* CV. Bintang Kharisma masih dalam tahap pengembangan yang bertujuan untuk mencegah terjadinya pencurian data yang dilakukan oleh peretas. Karena jika pencurian data terjadi dapat menyebabkan penyalahgunaan data untuk hal yang tidak diinginkan dan dapat merugikan para pelanggan dan juga perusahaan.

Sistem otentikasi *One Time Password* adalah salah satu dari berbagai macam cara untuk mengatasi serangan peretas pada sistem *login*. Algoritma yang akan digunakan pada penelitian akhir ini adalah MD5 (Message Diggest 5)dan SHA1 (Secure Hash Algorithm 1). Dipilihnya algoritma MD5 dikarenakan pemrosesan data yang cukup cepat karena hanya mengambil panjang data sebesar 128 bit. Dan dipilihnya algoritma SHA1 karena kebal terhadap *collision* (tabrakan paket data)[1].

Pada latar belakang yang telah dikemukakan, dapat diperoleh beberapa permasalahan yaitu, bagaimana meningkatkan keamanan proses *login* sistem agar pada saat *username* dan *password* berhasil diketahui oleh orang lain, *username* dan *password*, serta informasi penting pada *website* masih tetap aman. Dan bagaimana cara merancang dan menciptakan aplikasi otentikasi keamanan sistem *login* berbasis *mobile* yang mudah digunakan sekaligus dimengerti oleh pengguna.

Meningkatkan keamanan sistem *login website* menggunakan *One Time Password* dan merancang aplikasi berbasis *Android* dengan tampilan yang sederhana sehingga mudah digunakan oleh pengguna adalah tujuan dari penelitian ini. Kinerja dari One Time *Password* diimplementasikan terhadap smartphone android dengan cara meng-hashing-kan *username, password*, dan waktu menggunakan algoritma *Message Digest 5* dan *Secure Hash Algorithm 1*.

Adapun batasan masalah pada penelitian ini adalah algoritma yang digunakan untuk penelitian ini yaitu*MD5* dan *SHA1. Dansmartphone android* digunakan sebagai pengganti *token* dalam mengimplementasikan *one time password. Aplikasi* dikembangkan pada sistem operasi *android* versi *4.2 jelly bean* atau lebih tinggi.

## 2. METODE PENELITIAN

Dalam penyusunan penelitian ini penulis melakukan berbagai macam metode dengan cara mengumpulkan data atau informasi yang dibutuhkan. Metode yang dibutuhkan antara lain:

**a. Studi pustaka**

Yaitu mencari, memahami, dan mempelajari dengan seksama dari buku atau berbagai macam artikel yang berkaitan dengan *One Time Password*, SHA1, dan MD5. Serta menggali sumber-sumber pustaka lainnya yang juga berhubungan dengan topik ini, yang bisa juga didapat dari berbagai makalah, forum diskusi, textbook, pendapat ahli, jurnal, dan sebagainnya, baik media cetak maupun elektronik.

**b. Wawancara**

Yaitu upaya yang dilakukan untuk mendapatkan dan melengkapi data-data yang diperoleh dapat melalui wawancara meliputi pihak-pihak terkait di dalam aplikasi *One Time Password* yang masih dalam tahap pembuatan.

**c. Prototyping**

Yaitu teknik analisis data dalam pembuatan perangkat lunak atau *software*.Dan teknik*Prototyping* merupakan proses pembuatan *dummy* atau model sederhana dari *software* yang akan dibuat, sehingga memungkinkan pengguna memiliki gambaran dasar tentang program untuk bahan evaluasi serta pengujian awal.Berikut tahapan dari model Prototyping :

1) Menentukan Kebutuhan

Bertemu dengan user yang akan membutuhkan aplikasi dengan mengidentifikasi permasalahan,lalu menentuhkan kebutuhan dan mencari konsep yang sesuai dengan yang dibutuhkan.

2) Merancang *Prototype*

Setelah garis besar konsep sudah disepakati, yang selanjutnya dilakukan membuat suatu *prototype* dengan cara membuat rancangan aplikasi yang bersifat sementara yang difokuskan pada garis besar konsep yang telah disepakati antara pengguna dan pengembang.

3) Evaluasi *Prototype*

User akan melakukan evaluasi dari *prototype* aplikasi, apakah aplikasi yang dibuat sudah sesuai dengan keinginan pengguna. Jika *prototype* sudah selesai maka langkah berikutnya akan diambil, namun jika tidak sesuai maka *prototype* akan diperbaiki dengan mengulang langkah pertama, kedua, dan ketiga.

4) Mengkodekan Aplikasi

Pada tahap ini, Prototyping aplikasi yang sudah disepakati dierjemahkan ke dalam bahasa pemrograman yang sesuai.

5) Menguji Aplikasi

Setelah aplikasi sudah menjadi suatu perangkat lunak yang siap pakai, aplikasi akan dilakukan pengujian terlebih dahulu untuk mengetahui ada atau tidaknya celah (bugs) pada fungsi utama aplikasi yang sedang dibuat.

6) Evaluasi Aplikasi

Pengguna akan melakukan evaluasi terhadap program atau aplikasi yang sedang dikembangkan, apakah aplikasi sudah sesuai dengan yang di harapkan. Jika telah sesuai maka langkah berikutnya akan dilakukan, namun jika dirasatidak sesuai yang diharapkan, aplikasi akan dirancang ulang kembali dengan mengulang langkah keempat dan kelima.

7) Menggunakan *Prototype*

Dilakukan pengembangan aplikasi yang sesuai dengan hasil evaluasi serta dilakukan penambahan atau perbaikan yang diminta oleh user ditahap sebelumnya. Jika telah sesuai dengan permintaan user, maka aplikasi dapat dikembangan menjadi aplikasi nyata.

**d. Pengujian**

Pada tahap ini dilakukan pengujian dari aplikasi yang telah dibuat, serta mengevaluasi apabila masih terdapat kesalahan dan kekurangan.

### 2.1. Serangan Keamanan Komputer

Cara seseorang untuk mendapatkan pesan dalam saluran komunikasi [2], penyerangan dapat dikategorikan menjadi:

**a. Sniffing**

Secara harfiah sniffing memiliki arti mencium, tentunya dalam hal ini yang dicium adalah data pesan (baik yang belum maupun yang sudah dienkripsi) dalam suatu saluran komunikasi. Hal tersebut umum terjadi pada saluran publik yang rentan keamanannya. Pelaku dapat merekam pembicaraan yang terjadi antara dua *user* atau lebih.

**b. Replay Attack**

Hacker bisa merekam pesan-pesan handshake (persiapan komunikasi), ia sangat mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak yang ada pada jalur komunikasi.

**c. Spoofing**

Penyerang, misalnya A, bisa menyamar menjadi B. Semua orang dibuat percaya bahwa A adalah B. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada yang salah dengan komunikasi yang sedang di lakukan, padahal komunikasi tersebut dilakukan dengan sang penipu/penyerang. PIN ke dalam *Card Acceptance Device* (CAD) yang benar-benar di buat seperti CAD asli tentu saja sang penipu bisa mendapatkan PIN pemilik smartcard. Pemilik smartcard tidak tahu bahwa telah terjadi kejahatan didalamnya.

**d. Man-in-the-middle**

Jika terkadang spoofing hanya menipu satu pihak, maka dalam scenario ini saat A hendak berkomunikasi dengan C, B dimata A seolah-olah adalah C, dan B dapat pula menipu C sehingga B seolah-olah adalah A. B dapat berkuasa dengan penuh atas jalur komunikasi keduanya dan bisa membuat berita fitnah atau hoax.

### 2.2 Metode Pengembangan Sistem

**a. One Time *Password***

One Time *Password* (OTP) adalah *password* yang hanya berlaku untuk satu kali sesi *login* atau transaksi. OTP menghindari sejumlah kelemahan yang berkaitan dengan tradisional (statis) *password*. Kelemahan paling penting yang ditujukan oleh OTP berbeda dengan *password* statis, OTP tidak rentan terhadap serangan *replay* (*replay attack*). Ini berarti jika penyusup memilliki potensi berhasil merekam OTP yang sudah digunakan untuk masuk ke dalam sistem atau layanan atau untuk melakukan transaksi, penyusup tersebut tidak akan dapat menyalahgunakannya disesi berikutnya karena kode OTP tidak berlaku lagi [3].

**b. Message Digest 5**

Message Digest Algorithm 5 atau MD5adalah fungsi hash kriptografi. Pada umumnya metode algoritma ini digunakan untuk melakukan pemeriksaan integritas file dalam berbagai macamsituasi[4]. Dalam Penelitian ini Algoritma MD5 digunakan sebagai salah satu proses *hashing* untuk pembangkit kode *OTP*.

**c. Secure Hash Algorithm 1**

Secure Hash Algorithm 1 atau SHA1 menerima masukan berupa *string* dengan ukuran maksimum 264 bit. Untuk setiap *string*, SHA1 akan menghasilkan keluaran sebanyak 160bit dari *string* tersebutdan *string* keluaran itu disebut *message digest*. Panjang jarak *message digest* dapat berkisar antara 160 sampai 512 bit tergantung algoritmanya. Berdasarkan cirinya SHA1 dapat dipadukan dengan algoritma kriptografi lainnya, seperti *Digital Signature Algorithms* atau dalam generasi angka yang acak (*bits*).SHA1 dikatakan cukup aman karena proses SHA1 dihitung secara infisibel untuk mencari *string* yang sesuai untuk menghasilkan *message digest* atau dapat juga digunakan untuk mencari dua*string* berbeda yang akan menghasilkan *message digest*yang sama. Untuk SHA1 ukuran blok*string* -m bit- dapat ditentukan tergantung dari algoritmanya. Pada SHA-1 masing-masing blok *string* mempunyai 512 bit dimana dapat dilakukan dengan 16 urutan sebesar 32 bit. SHA1 digunakan untuk menghitung *message digest* pada*string* atau *file* data yang diberikan sebagai *input*. Tujuan pengisian *string* adalah untuk menghasilkan total dari *string* yang diisi menjadi perkalian dari 512 bit[5].

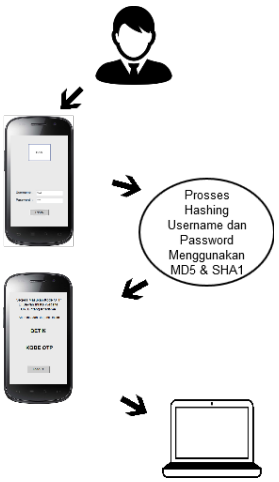
## 3. RANCANGAN SISTEM DAN APLIKASI

Pada penelitian ini akan dibuat dua aplikasi yaitu aplikasi *login* web dan aplikasi untuk membangkitkan One Time *Password* pada smartphone berbasis Android. Proses dari aplikasi yang akan dibuat dimulai dari pengisian *username* dan *password* yang telah terdatakepada aplikasi Android. Pada aplikasi Android akan dihasilkan

*generate code* yang akan digunakan untuk mengisi form sebagai kode One Time *Password* pada website. User dapat masuk (*login*) pada website dengan memasukkan *username*, *password*, dan kode generate yang sudah didapatkan dari Android lalu memilih *button login*.

### 3.1. Alur Proses*One Time Password*

Pada alur proses *login website* dilakukan pengecekan *username* dan *password,* apakah sudah seperti data yang terdaftar pada database atau belum. Jika sudah sesuai maka kode OTP dengan estimasi waktu 60 detik akan ditampilkan. Jika lebih dari 60 detik maka mobile akan melakukan *generate* kode *OTP* baru. Apabila semua proses tersebut sudah berjalan sistem akan melakukan validasi proses *login* berhasil atau gagal, dan menampilkan pesan dalam bentuk *message box* atau *popup*.




*Gambar 1: Alur Proses One Time Password*

### 3.2. Rancangan Layar Menu *LoginMobile*

Pada tahap pertama pengguna memasukkan *username* dan *password* pada kolom yang tersedia dengan catatan *username* dan *password* sudah terdaftar pada *database* untuk mendapatkan kode *OTP* yang akan ditampilkan pada *mobile android*.




*Gambar 2: Rancangan Layar Menu LoginMobile*

### 3.3. Rancangan Layar *Mobile One Time Password* Dibangkitkan

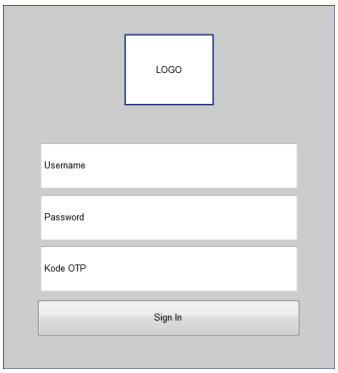
Kode *OTP* akan tampil setelah proses *login* sebelumnya dinyatakan berhasil. Kode OTP akan tampil dan berganti setiap 60 detik sekali. Kemudian kode dapat diinputkan pada *Text Field* Kode OTP yang tersedia pada halaman *loginwebsite*.




*Gambar 3: Rancangan Layar MobileOne Time Password Dibangkitkan*

### 3.4. Rancangan Layar Form *Login Website*

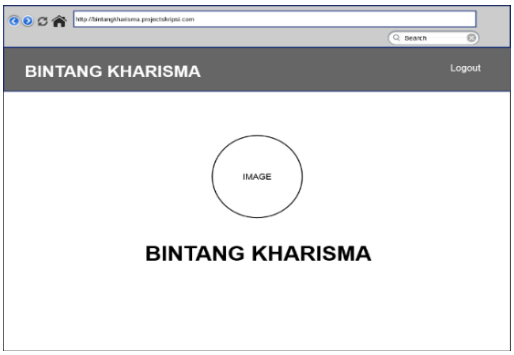
Berikut merupakan menu yang akan tampil pada website dan yang akan digunakan untuk memasukkan *Username*, *Password* dan kode OTP yang telah didapatkan dari mobile token pada proses sebelumnya. Setelah itu sistem akan melakukan pengecekan terhadap database dan kode OTP antara *client* dan *server.*Proses pengecekan kode OTP sangat berpengaruh terhadap koneksi dan waktu anata *client* dan *server.*




*Gambar 4: Rancangan Layar Form Login Website*

### 3.5. Rancangan Layar Halaman Utama *Website*

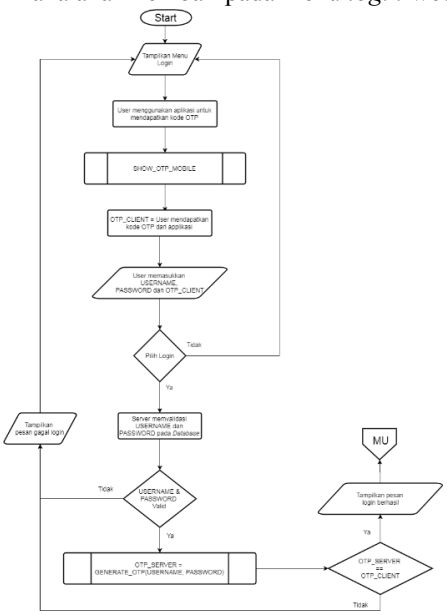
Berikut merupakan tampilan Menu Utama *Website* setelah proses *login* atau proses validasi antara *client* dan *server* yang sebelumnya berhasil dilakukan. Halaman ini tidak akan tampil jika proses *login* OTP tidak berhasil, dengan kata lain kode user ID atau kode OTP tidak diterima oleh sistem.




*Gambar 5: Rancangan Layar Halaman Utama Website*

### 3.6. *Flowchart Login Website*

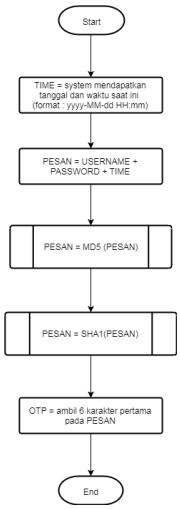
Pada Flowchart ini menggambarkan proses *Login* pada web. Untuk masuk pada halaman utama web, user harus memasukkan *username*, *password* dan kode OTP yang didapatkan dari mobile token terlebih dahulu. Setelah itu sistem akan melakukan pengecekan *username*, *password*, dan kode otp apakah sudah sesuai. Jika sesuai maka akan menampilkan menu utama web, tetapi jika tidak sesuai maka akan kembali pada menu *login* web.




*Gambar 6: Flowchart Login Website*

### 3.7. *Flowchart One Time Password*

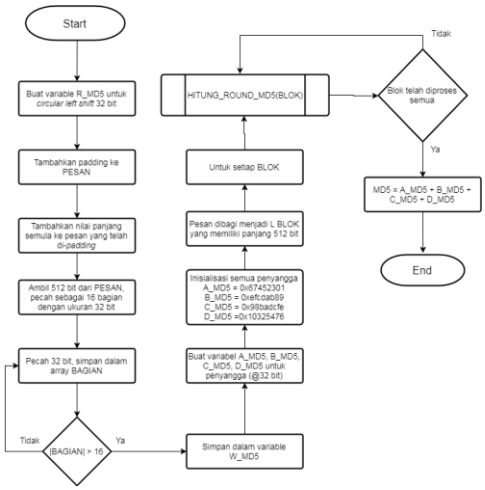
Pada flowchart berikut ini menjelaskan nilai OTP menggunakan satu variabel. Variable tersebut mengambil satuan waktu *login* yang diambil adalah jam, menit, tanggal, bulan, dan tahun. Kemudian variabel tersebut digabungkan dengan *username* dan *Password* pengguna user. Variabel ini akan di hashing dengan menggunakan algoritma Secure Hash *Algorithm 1 (SHA1)* dan *Message Diggest 5 (MD5)*. Ketika sudah mendapatkan 40 bit hasil hasing, kode akan disubstring 6 digit pertama dan disimpan sebagai variabel kode OTP. Setelah didapatkan kode OTP akan ditampilkan di menu mobile OTP pada android. Proses ini akan berlangsung setiap 60 detik sekali untuk mendapatkan kode OTP yang terbaru.




*Gambar 7: Flowchart One Time Password*

### 3.8. *Flowchart MD5*

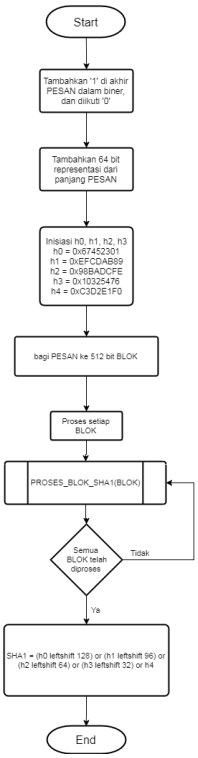
Pada flowchart berikut ini akan dijelaskan bagaimana proses hashing variabel yang menampung waktu *login, username* dan *password* menggunakan algoritma *Message Digest 5 (MD5)*.




*Gambar 8: Flowchart MD5*

### 3.9. *Flowchart SHA1*

Pada flowchart dibawah ini akan dijelaskan bagaimana proses hashing variabel yang menampung waktu *login, username* dan *password* menggunakan algoritma Secure Hash Algorithm (SHA1).




*Gambar 9: Flowchart SHA1*

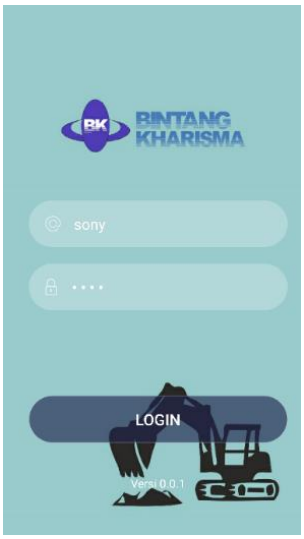
## 4. HASIL DAN PEMBAHASAN

### 4.1. Tampilan Layar Aplikasi

Tampilan layar program berguna untuk mengetahui apakah aplikasi yang telah dibuat sudah sesuai dan telah berjalan secara maksimal atau bahkan terjadi beberapa kesalahan yang tidak diinginkan. Dan tampilan layar juga berfungsi sebagai bahan untuk evaluasi peneliti terhadap program yang telah dibuat. Dengan dibuatnya tampilan layar juga memudahkan peneliti dan pembaca menganalisa keunggulan dan kekurangan program. Berikut ini adalah tampilan layar aplikasi baik pada smartphone android maupun tampilan layar pada website beserta penjelasan penggunaannya di masing-masing tampilan yang ada pada aplikasi One Time *Password* ini.

**a. Tampilan Layar Menu *Login* pada *Mobile***

Tampilan aplikasi pada *smartphone android* terdiri dari beberapa bagian, salah satunya tampilan awal ketika user meng-input kode *username* dan *password*. Ketika user telah mengisi *textfield username, password* dan menekan tombol *Login*. Sistem akan melakukan pengecekan apakah *username* dan *password* yang diinputkan sesuai dengan data yang tersimpan pada *database.* Berikut adalah tampilan ketika *user* melakukan penginputan *username* dan *password.*




*Gambar 10: Tampilan Layar Menu Login pada Mobile*

**b. Tampilan Layar Mobile*One Time Password* Dibangkitkan**

Pada gambar berikut ini adalah tampilan layar dimana ketika mobile token OTP dibangkitkan. Pada tampilan layar berikut ini juga terdapat waktu hitung mundur. Waktu mundur berfungsi mengingatkan user bahwa ketika waktu sudah habis akan muncul kode OTP baru. Pada tampilan layar ini juga terdapat kode OTP yang dapat digunakan untuk *login* pada website.

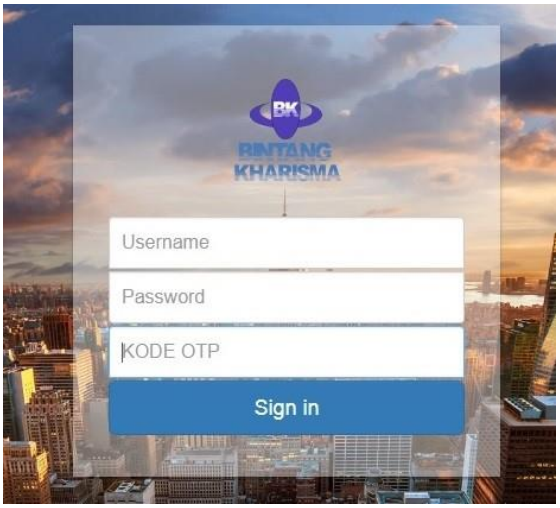



*Gambar 11: Tampilan Layar Mobile One Time Password Dibangkitkan*

**c. Tampilan Layar *Login Website***

Pada tampilan layar menu *login* web berikut ini menjelaskan terdapat 3 kolom yang tersedia. Kolom-kolom tersebut antara lain kolom *username, password*, dan kode OTP. Pada kolom *username* dan *password*, user memasukkan *username* dan *password* yang user miliki yang sesuai dengan databse. Pada

kolom kode OTP, user memasukkan kode OTP yang didapat dari Mobile Token Android.




*Gambar 13 : Tampilan Layar Login Website*

**d. Tampilan Layar *Website* Setelah Proses *Login***

Berikut ini adalah tampilan halaman *website* perusahaan yang akan muncul setelah melakukan proses *login* pada halaman utama *website*. Pada halaman ini terdapat beberapa *button link* pada bagian *header website* seperti portofolio, *about, contact* dan *logout.*




*Gambar 14 : Tampilan Layar Website Setelah Proses Login*

## 4.2. Evaluasi Program

Berdasarkan hasil pengujian yang telah dilakukan pada penelitian, terdapat beberapa kelebihan dan kekurangan dari aplikasi ini. Adapun kelebihan dari aplikasi ini adalah dengan adanya pengamanan tambahan pada sistem *login* akan membuat *website* menjadi lebih aman, dikarenakan kode *OTP* yang digunakan selalu berubah-ubah dalam jangka waktu 60 detik sekali. Kode *OTP* yang digunakan hanya sekali pakai atau tidak dapat digunakan kembali pada sesi berikutnya. Pembangkit kode *OTP* menggunakan *smartphone android* sebagai token yang hampir dimiliki oleh semua pengguna. Menggunakan Algoritma *MD5* dengan penambahan Algoritma *SHA1* yang bersifat *Hash* atau sekali pakai.

Sedangkan kekurangan yang terdapat pada aplikasi ini yaitu aplikasi hanya dapat digunakan atau diimplementasikan pada *smartphone* dengan sistem operasi *Android,* dan juga keberhasilan pembangkitan kode OTP dipengaruhi oleh koneksi dan perbedaan waktu antara client dan server.

## 4.3. Analisa Hasil

Proses *login* pada website melakukan pengecekan antara *client* dan *server* meliputi *username, password* dan kode OTP dan menampilkan validasi dalam bentuk *message box* atau *popup*. Dari proses yang telah dilakukan dapat disimpulkan bahwa kode OTP menjadi salah satu bagian terpenting untuk dapat melakukan *login* ke halaman utama website. Hal ini karena tersedianya kolom kode OTP pada halaman *login* website yang harus diisi dengan kode OTP yang didapat dari aplikasi Mobile Token.

Pengujian juga dilakukan dengan meng-install-kan perangkat lunak untuk sniffing yaitu keylogger. Dengan asumsi bahwa *database* telah diretas, peretas berusaha melakukan *login* kembali menggunakan *username* dan *password* yang telah didapatkan, kode OTP sudah tidak berlaku lagi karena kode OTP berubah secara otomatis setiap 60 detik. Dengan adanya masa aktif yang dimiliki kode OTP maka setelah kode OTP sudah melewati 60 detik atau kode OTP sudah pernah digunakan untuk mengakses sistem maka status dari kode OTP menjadi tidak valid. Jika kode OTP tidak valid maka user tidak dapat mengakses website.

Berikut ini dijelaskan hasil pengujian aplikasi OTP dengan menggunakan dua *username* yang berbeda secara berulang-ulang:

*Tabel1 : Hasil Pengujian*

| *Username* | *Password* | Kode OTP | Waktu/Jam | Status |
|---|---|---|---|---|
| **Sonny** | 1234 | 8D24F3 | 14:05:20 | Berhasil |
| **Sonny** | 1234 | 8D24F3 | 14:06:15 | Gagal |
| **Sonny** | 1234 | 518E85 | 14:06:40 | Berhasil |
| **Helmas** | 2234 | 3C98BF | 14:30:10 | Berhasil |
| **Helmas** | 2234 | D87D0E | 14:31:15 | Berhasil |
| **Helmas** | 2234 | 4C3F5F | 14:32:45 | Berhasil |

# 5. KESIMPULAN

## 5.1. Kesimpulan

Dari hasil pengujian dan implementasi yang sudah dilakukan, didapatkan beberapa kesimpulan yaitu, Algoritma *MD5* dan *SHA1* yang digunakan pada penerapan *One Time Password* dapat mengamankan sistem *login website* dengan cara memanfaatkan *Smartphone Android* sebagai pengganti token untuk mengimplementasikan *One Time Password.* Dan pengujian keamanan dari aplikasi yang telah dibuat dengan menggunakan cara

*sniffing* didapatkan hasil bahwa apabila *username* dan *password* berhasil diketahui atau disadap oleh orang lain, orang tersebut tidak dapat menggunakannya kembali untuk mengakses sistem *login*. Dengan demikian dengan adanya aplikasi *One Time Password* sistem *login website* terbukti menjadi lebih aman dari serangan peretas atau hacker.

### 5.2. Saran

Masih terdapat beberapa kekurangan pada penelitian ini, sehingga penelitian ini masih dapat dikembangkan dan diperbaharui. Saran penulis untuk penelitian atau untuk dikembangkan lebih lanjut, yang dapat dilakukan adalah menggunakan tambahan atau kombinasi algoritma lain untuk membangkitkan kode *OTP*, dan aplikasi ini diharapkan dapat dikembangkan untuk digunakan pada smartphone dengan sistem operasi lain seperti *iOS*, *Windows Phone*, dan berbagai sistem operasi lain yang mungkin saja akan dibuat pada era selanjutnya.

## 6. DAFTAR PUSTAKA

[1] Nugroho, E.P., 2016. SMS authentication code generated by Advance Encryption Standard (AES) 256 bits modification algorithm and One time *Password* (OTP) to activate new applicant account.International Conference on Science in Information Technology, 1(1), pp.40–44.

[2] Santoso, 2013. Dua Faktor Pengamanan *Login* Web Menggunakan Otentikasi One Time *Password* Dengan. In Semarang, pp. 204–210.

[3] Aryasa, K. & Paulus, Y.T., 2014. Implementasi Secure Hash Algorithm-1 Untuk Pengamanan Data Dalam Library Pada Pemrograman Java. , 1(1), pp.57–66.

[4] Mustofa, R.P., 2013. Aplikasi Mobile Android "One Time *Password*(OTP)" Untuk Meningkatkan Keamanan Otentikasi. , pp.1–15.

[5] Fresdian, Yama. 2015. MD5 (Message Digest Algorithm 5). Ilmu Komputer. Vol.1, No.1