TEKNIK PENULISAN KARYA ILMIAH

BRAMANTIO RIZKI NUGROHO

NIM 09121001044

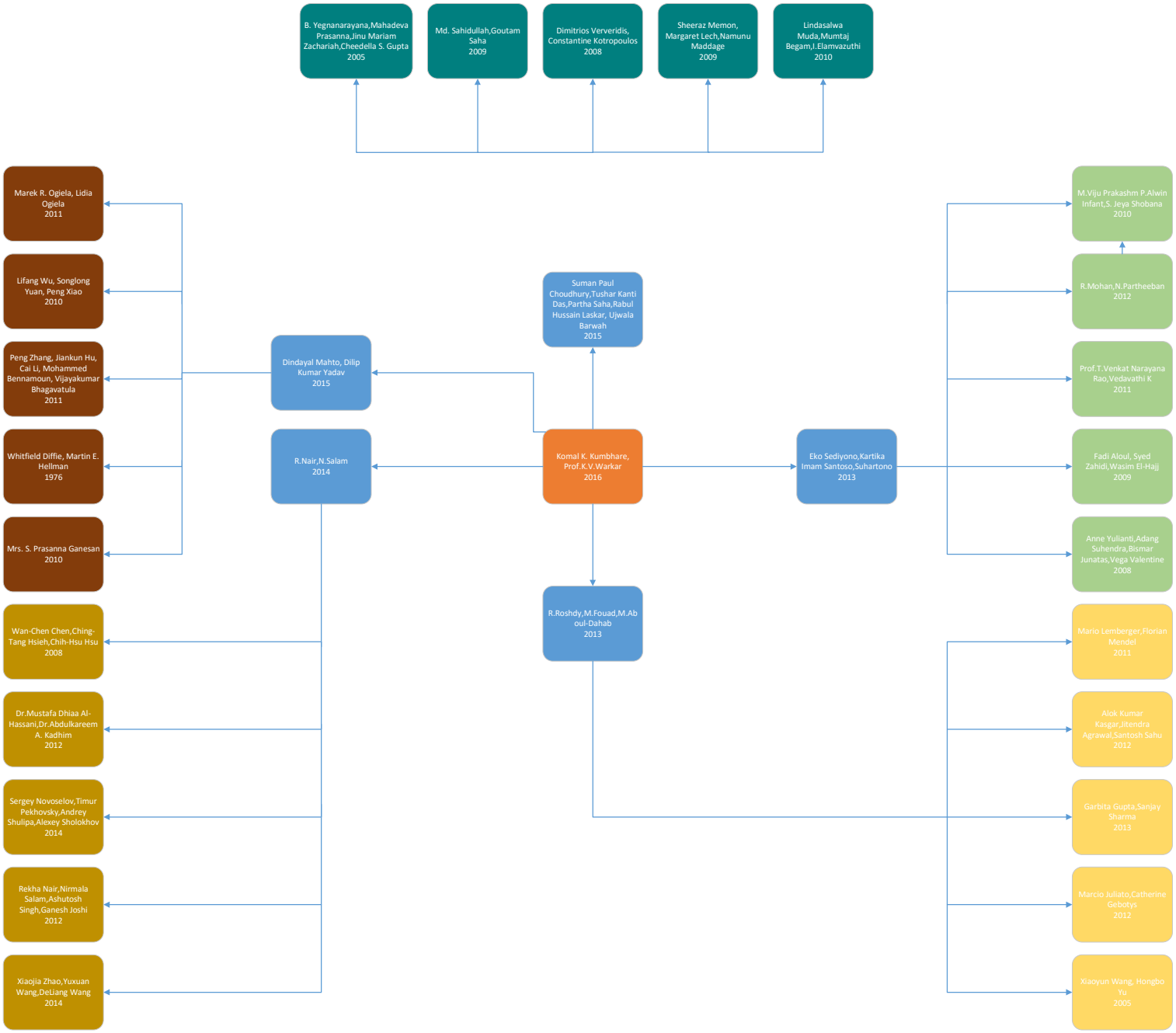
SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2015

A Review on Noisy Password, Voiceprint Biometric and One-Time-Password



A Review on Noisy Password, Voiceprint Biometric and One-Time-Password

Komal K. Kumbhare,Prof K V Warkar

Dalam paper ini membahas *Noisy password, voiceprint biometric dan one-time-password*. *Static Password* adalah metode yang paling sering digunakan dalam proses Otentikasi. *Dictionary attack, eve dropping, dan shoulder surfing* sangat mudah dilakukan pada password biasa. *Noisy password* bisa digunakan sebagai alternatif bagi *static password*. *Noisy password* mencoba mengatasi masalah-masalah yang disebutkan. Teknik *biometric* seperti *fingerprint, palm-vein scan*, dll bisa digunakan untuk *personal recognition*. Tapi jika dibandingkan teknik biometrik lainnya, voiceprint membutuhkan biaya yang lebih murah dalam implementasi. Aplikasi e-commerce menggunakan one-time-password untuk proses transaksi elektronik. Karena itu perlu menyediakan pengamanan saat mengirim one-time-password.

1. **Enhancing Security of One-Time Password using Elliptic Curve Cryptography with Biometrics for E-Commerce Applications (Dindayal Mahto & Dilip Kumar Yadav)**

   OTP digunakan untuk melawan tindak penyadapan. Penyadapan adalah salah satu jenis serangan pada lingkungan komputasi terhubung jaringan atau lingkungan komputasi yang terisolasi. Untuk mencapai 112 bit tingkat keamanan, algoritma Rivest Shamir dan Adleman (RSA) memerlukan kunci berukuran 2048 bit, sementara: kriptografi kurva elips (ECC) memerlukan kunci berukuran 224-255 bit. Masalah lain kebanyakan mengenai pelaksanaan model keamanan adalah penyimpanan kunci rahasia. Kunci kriptografis sering disimpan dengan cara en-secured yang tidak hanya dapat ditebak/rekayasa-sosial atau diperoleh melalui *brute force attack* (mencoba segala kemungkinan kombinasi password yang ada pada wordlist). Ini menjadi sebuah kelemahan dan memicu masalah integritas data dalam model keamanan. Untuk mengatasi masalah diatas, biometrik dikombinasikan dengan kriptografi untuk mengembangkan model keamanan yang kuat. Paper ini menyarankan peningkatan model keamanan sistem One-Time-Password menggunakan ECC dengan palm-vein biometrik. Model ini juga menyarankan keamanan yang lebih baik dengan ukuran kunci lebih kecil daripada kunci kripto-model umum lainnya. Kunci kriptografis juga tidak diharuskan untuk mengingat atau menyimpan, kunci-kunci ini diciptakan hanya saat diperlukan.

2. **New Directions in Cryptography (Whitfield Diffie & Martin E Hellman)**

   Perkembangan aplikasi teleprocessing telah membangkitkan kebutuhan terhadap jenis baru dari sistem kriptografi, yang meminimalkan kebutuhan akan saluran distribusi kunci keamanan dan penyediaan kesetaraan terhadap tanda tangan tertulis. Paper ini membahas cara-cara untuk memecahkan masalah yang terjadi saat ini. Termasuk juga membahas bagaimana teori-teori komunikasi dan komputasi mulai menyediakan alat bantu untuk memecahkan masalah kriptografi yang sudah berlangsung lama.

3. **A Novel Key Generation Cryptosystem Based on Face Features (Lifang Wu, Xingsheng Liu ,Songlong Yuan, Peng Xiao)**

Metode kriptografi sederhana mengharuskan pengguna untuk mengingat kunci, hal ini sangat menyulitkan. Teknik Biometrik berbasis kunci kriptografi menghasilkan kunci kriptografi biometrik secara langsung. Dalam paper ini, sebuah biometric cryptosystem berdasarkan pada face biometrics. Pada tahap enkripsi, 128-dimensional principal component analysis (PCA) fitur vektor pertama kali didapat dari gambar wajah. Dan 128 bit vektor biner diperoleh dengan cara *thresholding*. Kemudian kita memilih bit pembeda untuk membentuk bio-key dan nomor bit optimal disimpan di tabel *look-up*. Selain itu, *error-correct-code (ECC)* diperoleh dari menggunakan Reed-Salomon Algoritma. Pesan dienkripsi menggunakan *symmetric* DES dengan bio-key. pada fase dekripsi, 128-*dimensional principal component analysis* (PCA) fitur vektor dihasilkan dari query gambar wajah. Kemudian bio-key diciptakan menggunakan look-up table pada tahap enkripsi. Kunci akhir didapat baik menggunakan bio-key dan error-correct-code (ECC). Akhirnya, algoritma symmetric DES diterapkan untuk mendapatkan pesan menggunakan kunci akhir. Skema yang diusulkan ini diuji dengan menggunakan ORL face database, hasil percobaan menunjukkan bahwa algoritma yang digunakan efektif.

4. **A Reliable Speaker Verification System Based on LPCC and DTW (Rekha Nair & Nirmala Salam)**

Suara manusia dapat digunakan sebagai password dalam banyak layanan. Suara ini digunakan untuk memverifikasi suara pengguna dalam system verifikasi suara pengguna yang berbasis ekstraksi fitur dari sinyal suara. Dalam verifikasi suara pengguna otomatis, sinyal suara pengguna di proses untuk ekstrak informasi suara spesifik pengguna yang digunakan oleh voiceprint dan tidak bisa ditiru dari sumber apapun kecuali suara asli pengguna. System otomatis verifikasi suara pengguna yang berbasis LPCC (Linear Predictive Cepstral Coefficient)

dan DTW (Dynamic Time Warping) yang memiliki asumsi bahwa bentuk saluran vocal mengatur sifat suara yang dihasilkan.

5. **Robust Speaker Identification in Noisy and Reverberant Conditions (Xiaojia Zhao,Yuxuan Wang,DeLiang Wang)**

   Kekuatan system pengenalan suara pengguna sangat krusial dalam aplikasi nyata, dimana setidaknya terdiri dari additive noise dan room reverberation. Namun, efek kombinasi dari additive noise dan convolutive reverberation jarang dipelajari dalam Speaker Identification (SID). Ada dua tahap yang akan dibahas. Pertama, menghilangkan background noise langsung dari binary masking menggunakan deep neural netwok classifier. Lalu melakukan robust SID dengan model pembicara yang terlatih pada kondisi gema tertentu menggunakan batasan marginalization dan masking langsung. Hasil evaluasi menunjukan bahwa tujuan system secara substansi meningkatkan peforma SID diatas system relasi dalam jangkauan luas dari waktu gema dan rasio signal-to-noise.

6. **A pitfall in fingerprint bio-cryptographic key generation (Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, Vijayakumar Bhagavatula)**

   Inti dari bio-cryptography terletak pada stabilitas penciptaan kunci kriptografi dari biometrik tak pasti. Hal ini penting untuk meminimalkan munculnya ketidak pastian selama proses ekstraksi biometric feature. Dalam ekstraksi fingerprint feature, transformasi pixel-level image rotation adalah proses transformasi yang tidak efektif. Dalam paper ini, penyelidikan telah dilakukan terhadap analisis mekanisme dasar proses fingerprint image rotation dan efek potensial terhadap fitur utama, detail dan titik tunggal dari fingerprint transformed rotation. Kualitatif dan analisis kuantitatif telah disediakan berdasarkan percobaan intensif. Pengamatan bahwa integritas informasi dari gambar sidik jari asli bisa secara signifikan diganggu/dipalsukan dengan proses transformasi perputaran gambar, sehingga dapat menyebabkan titik tunggal

terlihat berubah dan menghasilkan sejumlah detail palsu yang diabaikan. Ditemukan bahwa proses kuantisasi dan interpolasi dapat mengubah fitur sidik jari secara signifikan tanpa mempengaruhi gambar visual. Eksperimen menunjukkan bahwa hingga 7% bio-cryptographic key bit kunci dapat terpengaruh akibat adanya transformasi rotasi.

7. **An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography (Mrs. S. Prasanna Ganesan)**

Sebagian besar aplikasi e-commerce dirancang menggunakan kriptografi asimetrik untuk menjamin otentikasi dari pihak-pihak yang bersangkutan. Sebaliknya, peningkatan permintaan untuk perangkat mobile telah menunjukkan pergeseran ke arah aplikasi mobile e-commerce. Penelitian ini menekankan bahwa protokol otentikasi yang ada, berdasarkan pada RSA asymmetric cryptography tidak cocok untuk perangkat tersebut karena keterbatasannya dalam daya komputasi, kapasitas memori, ukuran kunci dan dukungan kriptografi. Untuk alasan itu, protokol yang efisien untuk platform sumber daya yang terbatas yang mencapai tingkat keamanan sama dengan yang dicapai oleh protokol yang saat ini dirancang dan diterapkan. Protokol ini didasarkan semata-mata pada kriptografi elliptic curve asymmetric dan hasil menunjukkan bahwa kinerja yang dicapai baik berbeda dengan RSA.

8. **Image Based Crypto-Biometric Key Generation (Marek R. Ogiela, Lidia Ogiela)**

Kebutuhan/tuntutan Identitas dalam sistem informasi dapat terpenuhi dengan integrasi teknologi biometrik menggunakan algoritma kriptografi. Dalam hal ini, salah satu yang paling utama adalah seperangkat kunci kriptografi yang kuat dihasilkan dari berbagai jenis biometrik. paper ini menjelaskan beberapa solusi dalam lingkup ini berfokus pada pendekatan efisien untuk menghasilkan kunci kriptografi dari pola visual yang mengandung informasi pribadi. Menciptakan kunci kriptografi mungkin diidentifikasi oleh pengguna fitur, dan digunakan oleh

orang-orang tertentu. Secara khusus, kunci perangkat menggunakan palm-image dan coronary vessels akan disajikan.

9. **An Efficient Method for Additive and Convolutive Noise Reduction (Rekha Nair,Nirmala Salam,Ashutosh Singh,Ganesh Joshi)**

Seperti yang diketahui peforma dari system pengenalan suara pengguna otomatis mengalami penurunan karena kehadiran noise. Penurunan dari suara juga karena kehadiran additive background noise dan convolutive noise mengakibatkan beberapa kesulitan komunikasi. Paper ini membahas reduksi untuk additive dan convolutive noise saat berbicara.

10. **How to Break MD5 and Other Hash Functions (Xiaoyun Wang , Hongbo Yu)**

MD5 adalah salah satu fungsi hash kriptografi yang paling banyak digunakan saat ini. dirancang pada tahun 1992 sebagai perbaikan MD4, dan tingkat keamanan nya banyak dipelajari sejak itu oleh beberapa penulis. Sejauh ini hasil Terbaik yang dikenal adalah semi free-start collision, di mana awal nilai fungsi hash digantikan oleh nilai non-standar, yang merupakan nilai dari serangan. Dalam paper ini kami menyajikan serangan baru yang kuat pada MD5 yang memungkinkan kita untuk menemukan tabrakan secara efisien. Kami menggunakan serangan ini untuk menemukan tabrakan dari MD5 dalam waktu sekitar 15 menit sampai satu jam. Serangan tersebut adalah serangan diferensial, tidak seperti serangan diferensial pada umumnya, tidak menggunakan ukuran perbedaan, tetapi sebagai gantinya menggunakan modular integer substraction sebagai ukuran. Kita sebut ini sebagai modular diferensial. Aplikasi serangan terhadap MD4 dapat menemukan tabrakan dalam waktu kurang dari sepersekian detik. Serangan ini juga berlaku untuk fungsi hash lainnya, seperti RIPEMD dan HAVAL.

11. **Higher-Order Differential Attack on Reduced SHA-256(Mario Lamberger, Florian Mendel)**

    Dalam paper ini, kami mempelajari penerapan serangan diferensial tingkat tinggi pada fungsi hash. Kami menunjukkan bentuk kedua serangan diferensial pada fungsi kompresi SHA - 256 berkurang menjadi 46 dari 64 tahap. Kami menerapkan serangan dan memberikan hasil pada Tabel 1. Serangan terbaik sejauh ini (dalam model serangan berbeda-beda) dengan kompleksitas praktis adalah untuk 33 langkah dari fungsi kompresi .

12. **New Modified 256-bit MD5 Algorithm with SHA Compression Function (Alok kumar kasgar Jitendra Agrawal Santosh Sahu)**

    Dalam beberapa tahun terakhir, telah dilakukan penelitian signifikan lebih maju dalam analisis fungsi hash dan itu menunjukkan bahwa tidak ada algoritma hash yang cukup aman untuk tujuan kritis baik itu MD5 atau SHA-1. Saat ini para ilmuwan telah menemukan kelemahan-kelemahan dalam sejumlah fungsi hash, termasuk MD5, SHA dan RIPEMD jadi tujuan paper ini adalah kombinasi dari beberapa fungsi untuk memperkuat fungsi ini dan juga meningkatkan panjang kode hashhingga 256 yang membuat algoritma yang lebih kuat guna membuktikan tabrakan.

13. **Enhanced SHA-192 Algorithm with Larger Bit Difference (Garbita Gupta , Sanjay Sharma)**

    paper ini mencoba untuk mengembangkan sebuah algoritma kriptografi yang lebih kuat dan aman yang tidak hanya aman, tetapi juga mengurangi total waktu yang diperlukan dalam menyediakan integritas informasi. Fungsi hash diperkenalkan di kriptologi sebagai sebuah alat untuk melindungi integritas dari informasi. SHA-1 dan MD-5 adalah contoh di antara fungsi hash yang paling sering digunakan Para ilmuwan telah menemukan serangan tabrakan terhadap SHA-1, MD-5 untuk mengatasi ancaman dengan mencari titik lemah dari protokol bergantung pada hambatan tabrakan untuk keamanannya. Jadi untuk meningkatkan keamanan, SHA-192 ditampilkan di paper ini memiliki kemampuan mencerna pesan dengan panjang 192 bit dengan

perbedaan bit yang lebih besar. Untuk menciptakan perbedaan bit yang lebih besar, inti MD-5 dan SHA-1 digabungkan. Jadi solusi baru tidak akan rentan terhadap serangan tabrakan.

14. **Robust Speaker Identification Sstem Based on Two-Stage Vector Quantization (Wan-Chen Chen,Ching-Tang Hsieh,Chih-Hsu Hsu)**

    Paper ini menampilkan metode system identifikasi suara pengguna yang efektif. Berdasarkan wavelet transform, input dari sinyal suara diuraikan ke beberapa frekuensi bands, lalu LPCC (Linear Predictive Cepstral Coefficient) dari setiap band di kalkulasi. Selanjutnya, The Cepstral Mean Normalization Technique di diterapkan untuk semua fitur dihitung untuk menyediakan statistik parameter yang sama di semua lingkungan akustik. Supaya fitur multi-band speech berjalan secara efektif, disarankan multi-band 2-stage vector quantization (VQ) sebagai model pengenalan dimana perbedaan 2-stage VQ classifier diterapkan terpisah pada setiap band dan semua error dari 2-stage VQ classifiers dikombinasi untuk hasil semua error dan keputusan pengenalan global. Akhirnya database KING suara pengguna digunakan untuk evaluasi metode yang disarankan pada identifikasi suara pengguna text-independent. Hasil percobaan menunjukan bahwa metode yang disarankan memberi peforma yang lebih baik dari model pengenalan sebelumnya.

15. **Text-Dependent GMM-JFA System for Password Based Speaker Verification (Sergey Novoselov,Timur Pekhovsky,Andrey Shulipa,Alexey Sholokhov)**

    Paper ini mengusulkan New State-GMM Supervector Extractor untuk menyelesaikan masalah dari text-dependent speaker recognition. Skema yang diusulkan membuat ekstrasi supervector lebih muda untuk penerapn text-dependent JFA system pada verifikasi sandi. Kondisi semua dari global dan sandi text-prompted diperiksa. Percobaan dilakukan di Well Fargo Bank speech database menunjukan bahwa metode yang diusulkan memungkinan untuk

membuat model statistic lebih akurat dari sinyal speech dan mencapai relative pengurangan sebesar 44% pada ERR.

16. **Speaker Verification Based on Different Vector Quantization Techniques With Gaussian Mixture Models (Sheeraz Memon,Margaret Lech,Namunu Maddage)**

    Paper ini mengilustrasikan evolusi dari state-of-the-art verifikasi suara pengguna dengan menyorot kontribusi dari informasi teoritis berbasis vector quantization technique. kami mengeksplor aplikasi asing dari 3 vektor quantization algorithms yang berbeda, K-Means, Linde-Buzo-Gray(LBG) dan information theoretic Vector Quantization (ITVQ) untuk verifikasi suara yang efisien. EM (Expectation Maximization) algorithm digunakan GMM membutuhkan nilai yang tinggi dari pengulangan. Paper ini membandingakan EM termasuk K-Means,LBG dan ITVQ algorithm yang sudah diuji. GMM-ITVQ algorithm adalah alternative yang paling efisien untuk GMM-EM. Hasil tersebut memberikan tingkat klasifikasi yang benar terhadap level yang sama pada GMM-EM. Akhirnya, performa benchmark mewakili sifat system percobaan pada NIST SRE corpora.

17. **Comparative Analysis of Two Different System's Framework for Text Dependent Speaker Verification (Suman Paul Choudhury,Tushar Kanti Das, Partha Saha,Rabul Hussain Laskar, Ujwala Baruah)**

    Verifikasi suara adalah proses yang secara otomatis me-otentikasi identitas dari suara yang terproteksi dari sumber yang mengkontrol akses tersebut. Biasanya identitas di klaim dengan unik, posesi personal, pada kasus ini memakai suara pengguna. Paper ini menampilkan 2perbedaan kerangka untuk text-dependent speaker verifikasi. Satu menggunakan hard threshold based system dan Cohort Based System. System menggunakan MFCC dan DTW untuk tujuan verifikasi. Database dari 30 suara dikumpulkan di noisy environtment untuk pengujian dan validasi modul. Hasil percobaan menunjukan Sistem Verifikasi Cohort Based Speaker

memncapai peforma yang bagus dibandingkan Hard Threshold System. akhirnya sistem gabungan berdasarkan skor kinerja ternormalisasi dari individual technique melebihi stand-alone system dan meningkatkan kinerja untuk 85,61% untuk kondisi practical noisy.

18. **On The Use of Distributed DCT in Speaker Identification (Md. Sahidullah,Goutam Saha)**

    Fitur ekstraksi adalah tahapan yang paling signifikan dalam perkembangan Speaker Identification (SI). Banyak Sistem SI menggunakan mel-frquency cepstral coefficient (MFCC) sebagai parameter sinyal suara. MFCC diekstraksi langsung ke spectral weighting oleh bank of overlapping triangular filter diikuti dengan proses de-correlation. Biasanya, Discrete Cosine Transform (DCT-II) digunakan pada de-correlation. Paper ini menyarankan penggunaan de-correlation algorithm yang lebih baik untuk MFCC. Hasil percobaan pada 2 database public yang tersedia, dimana setiap pembicara menunjukan bahawa metode yang diusulkan meningkatkan kinerja baseline MFCC based SI system untuk bermacam angka.

19. **Voice Recognition Algorithms using Mel Frequency Cepstral Coefficient (MFCC) and Dynamic Time Warping (DTW) Techniques (Lindasalwa Muda, Mumtaj Begam,I.Elamvazuthi)**

    Algoritma Pemroresan Digital pada sinyal suara dan pengenalan suara sangat penting untuk kecepatan dan akurasi teknologi otomasi pengenalan suara. Karena itu proses sinyal digital sebagai fitur ekstraksi dan fitur pencocokan dikenalkan pada sinyal suara. Beberapa metode seperti Liner Predictive Coding(LPC), Hidden Markov Model(HMM),Artificial Neural Network(ANN) dan sebagainya dipakai untuk medapatkan identitas dengan mudah dan efektif. Proses ekstraksi dan pencocokan dijalankan tepat setelah pre-processing / pemfilteran sinyal dilakukan. Metode non-parametric untuk memodelkan human auditory perception system, mel frequency cepstral coefficients (MFCCs) dimanfaatkan pada teknik ekstraksi. Urutan non linear diketahui sebagai Dynamic Time Warping (DTW) dikenalkan oleh Sakoe Chiba telah digunakan sebagai fitur teknik pencocokan. Jelas bahwa sinyal suara cenderung memiliki temporal rate

yang berbeda, barisnya penting untuk membuat kinerja yang lebih baik. Paper ini menunjukkan kelangsungan MFCC untuk ekstrak fitur dan DTW untuk menguji pola-pola.

20. **Gaussian Mixture Modelling by Exploiting The Mahalanobis Distance (Dimitrios Ververidis, Constantine Kotropoulos)**

    Algorithm Expectation-Maximization(EM) untuk gabungan model Gaussian yang ditingkatkan melalui pengujian 3 statistik. Pengujian pertama multi-variasi normalisasi standar berbasis jarak Mahalanobis dari contoh pengukuran vector dari komponen Gaussian Center tertentu. Test ini menggunakan urutan untuk memperoleh keputusan apakah membagi komponen ke 2 atau tidak. Pengujian kedua adalah central tendency criterion berdasarkan observasi bahwa multi variasi kurtosis menjadi besar jika komponen dibagi ke 2 gabungan atau lebih sumber Gaussian dengan common centers. Jika hipotesis common center benar, komponen akan terbagi dalam 2 komponen baru dan pusatnya diinialisasi oleh kompenen lama untuk dibagi. Jika tidak, pembagian selesai oleh memperoleh deskriminan oleh pengujian ke 3. Pengujian ini berdasarkan fungsi distribusi kumulatif marjinal. Hasil percobaan menunjukan melawan 7 EM lainnya semuanya menghasilkan data-sets dan yang nyata. Percobaan ini menampilkan jika usulan EM mempunyai peningkatan kemampuan untuk mencari model utama, sambil menjaga waktu eksekusi yang singkat.

21. **Combining Evidence From Source, Suprasegmental and Spectral Features for a Fixed-Text Speaker Verification System (B. Yegnanarayana,S.R.Mahadeva Prasanna,Jinu Mariam Zachariah,Cheedella S.Gupta)**

    Paper ini mengusulkan text-dependent speaker verification system dimana menggunakan tipe yang berbeda dari informasi untuk membuat keputusan mengenai klaim identitas suara pengguna. Baseline system mengunakan teknik dynamic time warping(DTW) untuk pencocokan. Deteksi ucapan penting untuk kinerja DTW-based. Metode berdasarkan

vowel onset point (VOP) bertujuan untuk melacak ucapan. Metode yang disarankan untuk verifikasi suara menggunakan suprasegmental dan sumber fitur disamping fitur spectral. Fitur suprasegmental sebagai pitch dan durasi di ekstraksi menggunakan warping path information dalam algoritma DTW. Fitur dari

sumber eksitasi, diekstrak menggunakan model jaringan saraf, juga digunakan dalam sistem verifikasi speaker text-dependent. Meskipun suprasegmental dan sumber fitur individual mungkin tidak menghasilkan kinerja yang baik, menggabungkan bukti dari fitur ini tampaknya meningkatkan kinerja system secara signifikan. model jaringan saraf yang digunakan untuk menggabungkan bukti dari berbagai sumber informasi.

22. Secure Login by Using One-Time Password Authentication Based on MD5 Hash Encrypted SMS (Eko Sediyono,Kartika Imam Santoso,Suhartono)

Kombinasi One Time Password (OTP), SMS gateway dan algoritma enkripsi MD5 hash digunakan untuk pengembangan keamanan prosedur login untuk akses system informasi akademik berbasis web. Kode bisa di enkripsikan berupa ID mahasiswa, Nomor telefon, waktu akses. Sistem membutuhkan 3 menit untuk masuk aman dengan SMS-based OTP. Waktu tersebut memaksa dan mempersempit waktu peretas untuk menyusup. Delay waktu tersebut diperoleh dari survey dengan provider layanan di Indonesia. Kode dihasilkan dari system yang lebih baik dari Pseudo Random Number Generator (PRNG).

23. Multi Factor Authentication Using Mobile Phones (Fadi Aloul,Syed Zahidi,Wasim El-Hajj)

Paper ini menjelaskan metode pengimplementasian 2 faktor otentikasi menggunakan telfon seluler. Metode yang diusulkan menjamin bahwa layanan seperti online banking atau mesin ATM dengan cara yang sangat aman. System yang diusulkan menggunakan aplikasi telfon selular sebagai token untuk One Time Password generator. One Time Password yang dihasilkan

valid hanya untuk waktu pendek sesuai user dan dihasilkan oleh factor yang unik antara user dan telefon seluler itu tersebut.

24. **Modified Authentication using One Time Password to Support Web Services Security (Adang Suhendra,Anne Yulianti,Bismar Junatas,Vega Valentine)**

    Paper ini memberi informasi apa itu layanan web, resiko ang akan terjadi, dan beberapa teknik pengendalian keamanan layanan web. Paper ini juga mengusulkan rancangan baru model otentikasi dengan one-time password(OTP) generator dengan kode java, sebagai teknik mempertahankan keamanan.

25. **Design and Implementation a New Security Hash Algorithm Based on MD5 and Sha-256 (R.Roshdy,M.Fouad,M.Aboul-Dahab)**

    Fungsi hash kriptografi mempunyai peran penting di kriptografi untuk mencapai tujuan keamanan tertentu diantarana untuk authenticity, digital signatures, digital time stamping, and entity authentication. Hal tersebut juga berhubungan kuat dengan tools kriptografi penting seperti block ciphers dan pseudorandom functions. Sebelumnya proposal baru keamanan hash algorithm berdasarkan kombinasi fungsi SHA-256 (secure Hash Algortihm 256) dengan modifikasi message expansion dan MD5(Message Digest 5) berdasarkan skema double-Davis-Mayer untuk mengatasi kelemahan fungsi ini. Algoritma hash telah didesain untuk memenuhi perbedaan tingkatan keamanan dan menolak serangan advanced hash dengan peningkatankompleksitas derajat algoritma hash yang diusulkan. Analisa keamanan dari algoritma yang diusulkan dibandingkan dengan SHA256 dan memberikan keamanan lebih dan hasil yang bisa diterima.

26. **Authentication Using Mobile Phone as a Security Token (Prof T Venkat Narayana Rao,Vedavathi K)**

    2 faktor otentikasi menggunakan elemen/alat sebagai token dan kartu atm. Untuk menyelasaikan masalah password dimana ketidaknyamanan user dan pengeluaran untuk layanan provider. Untuk menghindari penggunaan alat tambahan, telefon seluler bisa digunakan sebagai keamanan token. Di paper ini beberapa perbedaan solusi otentikasi menggunakan telefon selular sebagai otentikasi token dimana solusi ini berbeda di kompleksitas,kekuatan,keamanan, dan user friendliness. 1 dari skema otentikasi (OTP solution) diimplementasi untuk verifikasi kegunaannya. Karena itu, klasifikasi dan evaluasi dari perbedaan solusi yang disediakan sesuai kriteria.

27. **Design A Text-Prompt Speaker Recognition System Using LPC-Derived Features (Dr. Mustafa Dhiaa Al-Hassani, Dr. Abdulkareem A. Kadhim)**

    Manusia tidak lepas dari komputer setiap hari, dan komputer mengambil alih layanan yang seharusnya dilakukan langsung antar individu. Hal Ini mendorong berkembangnya sistem biometrik. Penggunaan informasi biometrik telah dikenal luas baik untuk identifikasi seseorang dan aplikasi keamanan. paper ini membahas penggunaan fitur pengguna untuk melindungi akses yang tidak diinjinkan. Sebuah sistem pengenalan pengguna untuk contoh pidato 6304 disajikan berdasarkan pada LPC-derived features. Kosakata dari 46 contoh pidato dibuat untuk pembicara 10, dimana setiap orang yang berwenang diminta untuk mengucapkan setiap contoh sebanyak 10 kali. Dua mode berbeda dianggap mampu mengidentifikasi individu menurut contoh pidato mereka. Dalam tahap identifikasi closed-set, ditemukan bahwa semua LPC derived features yang diuji memberikan hasil melebihi koefisien LPC dan 84% sampai 97% angka identifikasi tercapai. dengan Menerapkan langkah-langkah pra proses pada sinyal pidato (preemphasis, remove DC offset, frame blocking, overlapping, normalisasi dan windowing)

meningkatkan representasi speech features, dan hingga 100% angka identifikasi diperoleh dengan menggunakan pembobotan Linear Predictive Cepstral Coefficients (LPCC). Dalam mode verifikasi pengguna open-set dari model sistem yang diusulkan, sistem memilih secara acak sebuah frase dari 8-contoh yang ada di database untuk tiap percobaan yang ditampilkan pada sistem. hiingga 213 Uji text-prompt dari 23-pembicara berbeda (resmi dan tidak resmi) tercatat (yaitu, 1704 sampel) untuk mempelajari perilaku sistem dan untuk menghasilkan ambang optimal dimana para pembicara terverifikasi atau tidak ketika dibandingkan dengan referensi percobaan pengguna resmi pembicara dibangun dalam mode pertama, dimana hasil verifikasi terbaik diperoleh dengan tingkat lebih besar dari 99%

28. Eliminating Vulnerable Attacks Using OneTime Password and PassText – Analytical Study of Blended Schema (M. Viju Prakash, P. Alwin Infant and S. Jeya Shobana)

Jaringan aman sebagian tergantung pada otentikasi pengguna dan sayangnya skema otentikasi yang digunakan saat ini sama sekali tidak aman. Beberapa sandi tidak dominan, sehingga serangan brute force yang belum pernah terjadi sebelumnya menjadi berpotensi terjadi. Di sini kita telah merancang skema gabungan dari Algoritma One-Time-Password(OTP) digabungkan dengan PassText sehingga mempermudah penyimpanan dan handal. Hal ini cukup dan cepat bagi sistem, sementara pada saat yang bersamaan menyisakan celah untuk mengatasi serangan brute force. algoritma OTP yang didukung dengan ciri khas pengguna seperti International Mobile Equipment Identification and Subscriber Identification Module, menyebabkan alfanumerik token terbatas yang berlaku untuk satu sesi dan satu kali penggunaan. PassText adalah cara mudah untuk skema otentikasi system yang memungkinkan pengguna tidak harus untuk menghafal setiap password yang sulit atau kombinasi karakter. Rangkaian dari dua skema ini dua memberikan keamanan maksimum untuk otentifikasi dan hampir mustahil untuk ditembus. Kami juga telah mengusulkan ukuran baru dari tingkat

keamanan dari banyak skema otentikasi yang populer mengalahkan salah satu yang kami usulkan.

29. **A Quantitative Analysis of a Novel SEU-Resistant SHA-2 and HMAC Architecture for Space Missions Security (Marcio Juliato,Catherine)**

Peningkatan permintaan keamanan operasi misi luar angkasa telah menuntun ke munculnya mekanisme kriptografi di pesawat luar angkasa. Namun, aplikasi kriptografi sangat sensitive ke bit-flips karena radiasi-induced single event upsets (SEUs). Pendekatan biasa mengurangi SEUs aplikasi space mempunai triple modular redundanc(TMR). Namun, teknik tersebut mendatangkan overhead ang besar pada area dan kekuatan implementasi. Pendekatan ang efisian untuk mencapai toleransi kesalahan dalam secure hash standar (SHS) dan dalam keyed-hash message authentication code(HMAC). Saat membandingkan TMR tujuan skemanya tidak hana mencapai ketahanan tinggi terhadap SEUs, tapi juga mengurangi implementasi kebutuhan area dan konsumsi power. Hasil yang diperoleh terhadap field-programmable gate array (FPGA) menunjukan bahwa HMAC/SHA-512(Secure hash Algorithm) dalam rata rata 53% less area dan less power dibandingakan teknikTMR biasa. Selanjutnya memori dan register dari HMAC/SHA-512 module sekitar 171 dan 491 kali lebih tahan terhadap SEUs dari TMR. Penelitian ini penting untuk memungkinkan efisien nya mekanisme keamanan space system.

30. **Secure Multimodal Mobile Authentication Using One Time Password (R.Mohan, N.Partheeban)**

Masalah keamanan yang meningkat di semua bidang seperti Bank, aplikasi pemerintah, industri kesehatan, militer organisasi, lembaga pendidikan. Organisasi pemerintah menetapkan standar, lewat undang-undang dan memaksa organisasi dan badan-badan untuk mematuhi standar-standar dengan konsekuensi. Ada beberapa masalah terkait keamanan di berbagai

industri dengan hanya satu link biasa yang disandikan. Kebanyakan sistem saat ini bergantung pada password statis untuk memverifikasi identitas pengguna. Namun, sandi tersebut dilengkapi dengan manajemen masalah keamanan. Pengguna cenderung menggunakan password mudah ditebak. Menggunakan sandi yang sama di beberapa akun, menulis sandi atau menyimpannya pada alat mereka. Disisi lain, hacker memiliki banyak cara untuk mencuri password seperti Shoulder surfing, snooping, sniffing,guessing. beberapa cara 'tepat' untuk menggunakan sandi telah diajukan. Beberapa di antaranya sangat sulit untuk digunakan dan yang lain mungkin tidak memenuhi masalah keamanan perusahaan. Dua faktor otentikasi menggunakan perangkat seperti token dan kartu ATM telah diusulkan untuk memecahkan masalah sandi dan telah terbukti sulit untuk di hack. Dua faktor otentikasi (T-FA) atau (2FA) adalah sebuah sistem dimana dua faktor berbeda yang digunakan sebagai penghubung untuk mengotentikasi. Usulan metode menjamin otentikasi layanan, seperti Belanja online, dilakukan dalam cara yang sangat aman. Sistem melibatkan penggunaan algoritma OTP (One Time Password)yang termasuk password dinamis untuk cara kedua mengotentikasi. one-time-password menggunakan informasi yang dikirim sebagai SMS ke pengguna sebagai bagian dari proses login