Kerentanan Sistem Fingerprint Authentication dan Efek mereka

Artikel *di* International Journal of Ilmu Komputer dan Keamanan Informasi, · Maret 2018

2 penulis:

Jatiya Kabi Kazi Nazrul Islam Universitas

2 PUBLIKASI **1** KUTIPAN

SEE PROFIL

Md. Mijanur Rahman

Jatiya Kabi Kazi Nazrul Islam Universitas

32 PUBLIKASI **119** CITATIONS

SEE PROFIL

Kerentanan Fingerprint Authentication Sistem dan Efek mereka

Tanjarul Islam Mishu

MS Penelitian Mahasiswa, Departemen Ilmu Komputer & Teknik
Jatiya Kabi Kazi Nazrul Islam Universitas
Mymensingh, Bangladesh Email:
tanjarul26@gmail.com

Dr Md. Mijanur Rahman

Associate Professor, Departemen Ilmu Komputer & Teknik
Jatiya Kabi Kazi Nazrul Islam Universitas
Mymensingh, Bangladesh Email:
mijanjkkniu@gmail.com

Abstrak **- Keamanan sidik jari biometrik merupakan tantangan besar sekarang-a-hari, karena memiliki penerimaan di seluruh dunia. Dikompromikan template sidik jari dapat meningkatkan ancaman mengerikan kepada pemiliknya. Karena kerentanan sistem otentikasi sidik jari, masalah keamanan tentang sidik jari telah menjadi keprihatinan besar. Penelitian ini merangkum kerentanan sistem otentikasi sidik jari dan menyoroti jenis efek yang tersedia terhadap tantangan-tantangan. Ini mencakup banyak pengetahuan rahasia tentang keamanan template sidik jari. Karya ini merupakan upaya untuk memberikan pengetahuan kompak untuk komunitas riset tentang masalah keamanan mengenai sistem otentikasi sidik jari.**

Kata kunci: ***serangan;*** ***kerentanan;*** ***kriptografi; Fingerprint Template; Template Keamanan.***

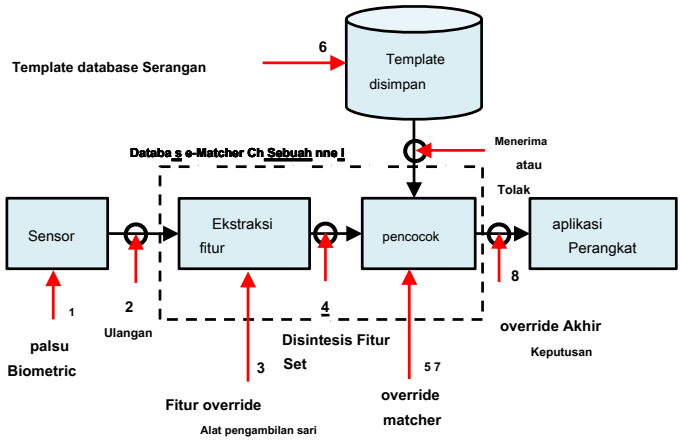
I. saya P ENDAHULUAN

sistem otentikasi sidik jari sangat populer di seluruh dunia karena keunikannya, kegunaan, kehandalan dll memiliki area aplikasi yang luas seperti kontrol perbatasan, bandara, bisnis, kesehatan, akses logis sistem, deteksi pidana, manajemen keamanan, ponsel pintar dll Jadi, keamanan daerah ini adalah masalah keprihatinan besar. Sebab, sistem ini rentan terhadap beberapa serangan. Ratha [1] disajikan model untuk kemungkinan serangan pada sistem biometrik. Model ini diperkenalkan varietas titik-titik rawan sistem. pekerjaan ini akan fokus pada poin yang disebutkan dalam model. Motif dari penelitian ini adalah untuk mendeteksi berbagai jenis serangan pada setiap titik model canggih ini dan juga untuk mengidentifikasi teknik keamanan yang ada untuk melindungi terhadap semacam serangan. Meskipun beberapa studi telah dilakukan selama serangan dan pendekatan keamanan, sebagian besar dari mereka berfokus pada serangan dan solusi secara terpisah. Sangat sedikit dari mereka yang pada kedua tetapi mereka tidak cukup. Mereka tidak mengekspos beberapa solusi langka yang ada.

Makalah ini disusun sebagai berikut. Ada delapan subbagian dalam Bagian 2. Setiap ayat pertama memperkenalkan serangan diikuti oleh solusi terhadap serangan. Sebagai serangan template database berisi data yang kaya, Bagian 2.6 adalah dibagi menjadi dua bagian. Akhirnya, kesimpulan ditarik dalam Bagian 3.

II. T ypes SEBUAH TTACKS ON F INGERPRINT S ystem

Ratha et al. [1] dan Anil et al. [2] menunjukkan delapan poin dari serangan dalam sistem biometrik (lihat Gambar-1). Setiap titik dan



Gambar 1. Tempat serangan dalam Sistem biometrik

serangan dan mengenai solusi telah dijelaskan dalam subbagian berikut.

A. Palsu Biometric

Sebuah palsu atau sidik jari buatan, yang disebut spoof, diberikan kepada scanner untuk mendapatkan akses ke sistem. Pemindai tetap tidak dapat membedakan antara palsu dan sifat-sifat asli. Jadi, penyusup dengan mudah mendapatkan akses ke sistem. [2] Putte dan Keuning [3] dibuat boneka sidik jari dengan dan tanpa kerjasama dari pemilik dan diuji pada beberapa sensor. Mereka menunjukkan hasil yang hampir setiap sensor menerima sidik jari boneka sebagai nyata pada upaya pertama. Matsumoto et al. [4] bereksperimen bergetah (palsu) jari pada 11 jenis sistem sidik jari yang berbeda. Dalam percobaan mereka, sekitar 68- 100 jari% bergetah diterima oleh sistem dalam prosedur verifikasi mereka. Mereka juga menunjukkan cara berikut bagaimana penyerang bisa menipu sistem pada scanner.

https://sites.google.com/site/ijcsis/ ISSN 1947-5500

(saya) Sidik jari Dikenal Sistem

Jari terdaftar sebenarnya disajikan pada scanner dengan cara jahat seperti kekuatan eksternal oleh penjahat, dengan menggunakan sidik jari ketika pengguna tidur dll

(Ii) Sidik jari tidak diketahui ke Sistem

Jika penipu dapat mengetahui tentang kategori sidik jari yang sebenarnya (uliran, lengkungan, loop dll), ia dapat menggunakan sidik jari yang sama tidak diketahui ke sistem. Meskipun hampir tidak mungkin, dapat membahayakan sistem yang dikembangkan atas dasar fitur cukup sidik jari. Ini mungkin efek pada False Acceptance Rate (FAR) dari sistem. Jadi, otentikasi harus didasarkan pada fitur yang cukup.

(aku aku aku) Terputus Sidik jari Dikenal

Hal ini mirip dengan sidik jari yang dikenal disebutkan sebelumnya. Tapi, itu adalah serangan yang mengerikan yang dilakukan oleh penjahat sampai parah sidik jari dari tangan pengguna nyata. Untuk dilindungi, kita harus mendeteksi adalah jari hidup atau tidak.

(Iv) Genetik Clone dari Sidik jari dikenal

kembar identik tidak memiliki sidik jari yang sama. Karena, pola sidik jari ditentukan oleh mekanisme genetik dan pertumbuhan saraf. Jadi, mereka tidak sama tetapi masih sangat dekat. Jadi, klon genetik dapat mencoba untuk menipu sistem. Untuk dilindungi dari jenis ancaman, kita harus menjaga melacak rekayasa genetik pada kemungkinan menciptakan klon.

(V) Buatan Clone dari Sidik jari dikenal

Penyerang dapat membuat dicetak sidik jari 3D atau dapat membuat cetakan dari jari dikenal dengan mana jari buatan dapat diproduksi.

(Vi) Dicetak Gambar dari Sidik jari Dikenal

Hal ini sangat mirip dengan yang sebelumnya. Dengan bantuan penyemprotan beberapa bahan di permukaan pemindai untuk merasa seperti jari yang sebenarnya, penipu dapat menggunakan dicetak citra sidik jari.

deteksi keaktifan dapat menjadi solusi untuk ciri-ciri biometrik palsu. Ada dua metode yang terpisah, seperti, pasif (non-merangsang) dan aktif (merangsang) metode deteksi keaktifan otomatis [5]. Umumnya, teknik deteksi pasif menggunakan probe biometrik direkam melalui sebuah sensor biometrik seperti pengukuran denyut nadi, pengukuran suhu, keringat aktif pori-pori deteksi, deteksi resistensi kulit, konduktivitas listrik dll [16] teknik deteksi aktif biasanya memerlukan interaksi tambahan yang harus diminta menggunakan prosedur tanggap tantangan. Pendekatan tantangan respon yang berbeda dapat digunakan seperti permintaan jari yang berbeda dalam urutan acak.

B. Replay Serangan

Setelah akuisisi data biometrik mentah, ia akan mengirimkan data mentah (misalnya sidik jari gambar mentah) ke modul ekstraksi fitur. penipu mencuri data mentah sifat biometrik oleh merebut saluran dan toko sifat tersebut. penipu dapat menjawab sifat biometrik yang tersimpan sebelumnya ke modul ekstraksi fitur untuk memotong sensor. gambar sidik jari yang dikirim melalui saluran biasanya dikompresi menggunakan WSQ. Karena standar kompresi terbuka, transmisi WSQ terkompresi gambar melalui Internet tidak terutama aman. Jika gambar dapat disita, dapat didekompresi dengan mudah yang dapat menyebabkan Replay Old data [1].

Teknik data bersembunyi seperti steganografi dapat diterapkan ketika gambar mentah dikirim ke fitur extractor.

C. Override Fitur Extractor

Para hacker, oleh Trojan Horse, mengambil kontrol atas ekstraktor fitur untuk menghasilkan set fitur karena mereka ingin [1].

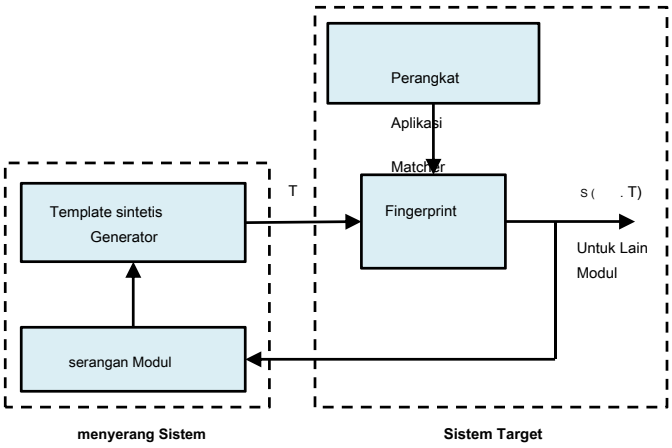
Ketika menginstal atau memperbarui program dalam perangkat itu harus diverifikasi dan harus menyadari menggunakan program pihak ketiga.

D. Disintesis Fitur Set

Jika penipu dapat mencegat saluran antara modul ekstraksi fitur dan matcher, dia bisa menggantikan set asli dengan disintesis fitur yang berbeda (dengan asumsi representasi diketahui penipu) [1]. saluran komunikasi yang tidak aman mungkin menghadapi 'Bukit Climbing Serangan' [2].

Bukit Climbing Serangan

Uludag & Anil telah mengembangkan menyerang untuk sistem otentikasi dasar sidik jari hal kecil [6]. Lokasi (c, r) dan orientasi Ɵ poin minutiae telah digunakan oleh serangan itu. Sistem akan bekerja sebagai penyerang tahu format template tapi tidak informasi dari template. Ia menggunakan skor pertandingan dikembalikan oleh matcher dan mencoba untuk menghasilkan set hal kecil yang menghasilkan nilai pencocokan berhasil tinggi untuk menjadi positif dalam identifikasi. Gambar-2 menggambarkan serangan Climbing Hill.



Gambar 2. Blok Diagram Hill Climbing Serangan

mengacu pada template database yang sesuai dengan pengguna *saya* . *i* = 1, 2,3, ... N, di mana N adalah jumlah total pengguna. aku s

https://sites.google.com/site/ijcsis/ ISSN 1947-5500

total jumlah hal-hal kecil di . T adalah sintetis template yang dihasilkan oleh sistem menyerang untuk pengguna *saya* . S (. T) adalah skor pencocokan antara dan T. mengacu pada ambang keputusan yang digunakan oleh pencocok. Perhatikan bahwa sistem menyerang tidak tahu nilai ini.

Pada awal serangan, itu menghasilkan beberapa template sintetis. Kemudian mulai menyerang dengan template ini dan mengumpulkan skor pencocokan dikembalikan oleh pencocok. Ia memilih template yang memiliki skor yang cocok tertinggi. Kemudian mencoba modifikasi (perturbing, menambahkan, mengganti atau menghapus hal kecil) untuk mendapatkan skor pertandingan yang lebih besar dan memilih yang lebih besar sebagai template terbaik T . Ini modifikasi berlanjut sampai pencocok menerima yang terbaik skor saat ini di mana () > .

Agar aman dari serangan mendaki bukit, kita dapat menambahkan beberapa fitur tambahan dalam matcher sistem otentikasi. Ini mungkin termasuk-

saya) pelacakan jumlah kegagalan dalam waktu tertentu.

ii) membatasi jumlah mencoba dalam waktu tertentu.

E. override matcher

Para hacker mengganti matcher dengan program kuda Trojan yang menghasilkan skor pencocokan sangat tinggi atau rendah sebagai hacker inginkan, terlepas dari skor original [1].

The Matcher juga program seperti fitur extractor. Serangan ke titik ini dapat diselesaikan dengan cara yang sama seperti fitur extractor dijelaskan pada bagian 2.3.

F. Template database Serangan

(saya) Jenis Serangan

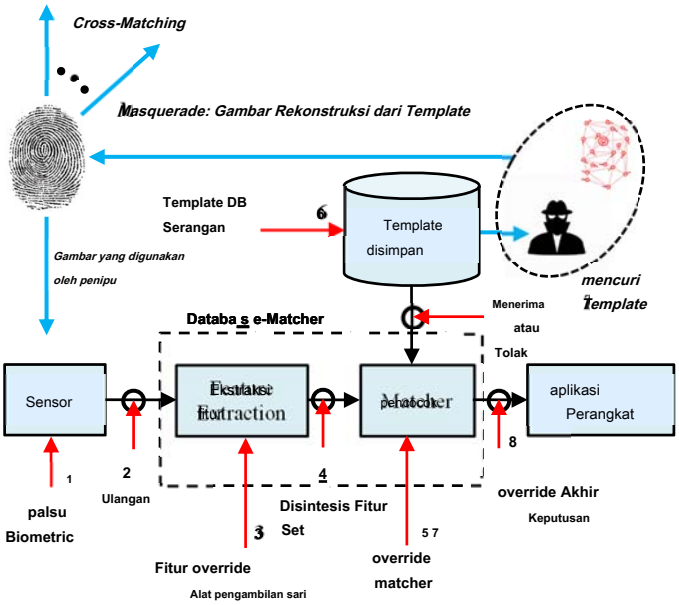
Database Template dapat menyebabkan tiga jenis ancaman [3] sebagai jelaskan di bawah.

Sebuah. Template Digantikan oleh Template The penipu ini

penipu dapat mengganti template asli dengan yang baru untuk mendapatkan akses tidak sah ke sistem kapan saja dia mau seperti pengguna yang berwenang.

b. Masquerade / Fisik Menipu dibuat dari template

Informasi detail unik untuk setiap individu. Pandangan non-rekonstruksi dominan dalam masyarakat biometrik, sampai beberapa penelitian baru-baru ini. Selama beberapa tahun terakhir, beberapa karya yang dilakukan yang menunjukkan bahwa gambar sidik jari dapat direkonstruksi dari template hal kecil. Gambar sidik jari direkonstruksi dari template hal kecil, yang dikenal sebagai "topeng" gambar karena bukan merupakan salinan dari gambar asli, kemungkinan akan menipu sistem ketika itu disampaikan [7]. Pada tahun 2007, Cappelli di al [8] melakukan beberapa eksperimen yang menakjubkan. Para penulis menganalisis ISO / IEC 19.794-2 hal kecil template standar. Mereka mengambil yang berbeda cara uji. Dalam satu eksperimen, mereka menggunakan hal-hal kecil dasar



Gambar 3. Gambar Rekonstruksi (Masquerade) dari template yang disimpan

Informasi saja (yaitu posisi x, posisi y, dan arah). Dalam tes lain, mereka juga digunakan opsional Informasi:. jenis hal-hal kecil, data yang Core dan Delta, dan data milik (bidang orientasi ridge dalam hal ini Dalam percobaan mereka, sembilan sistem yang berbeda diuji dan persentase rata-rata serangan yang sukses adalah 81% pada tingkat keamanan yang tinggi dan 90% di keamanan menengah tingkat. Gambar Rekonstruksi dengan poin serangan di sidik jari ditunjukkan pada gambar-3. Masquerade bisa sangat mengancam fakta kepada pemilik. Karena, hacker dapat melacak pemilik di mana ia / dia menggunakan sidik jari. Mereka mungkin hack Bank account dan akses yang aman lainnya. mereka mungkin menggunakan topeng untuk database di organisasi lain untuk mendapatkan akses yang tidak sah, meskipun mereka menggunakan template yang berbeda dan algoritma, yang disebut Cross-Matching.

c. Dicuri Template

Penipu bisa mencuri template dan memutar ulang bahwa pada matcher. template dicuri dapat digunakan sebagai disintesis set fitur.

(Ii) Teknik Perlindungan Template

Semua teknik perlindungan template yang dapat dikategorikan dalam dua kategori utama, seperti, (a) transformasi fitur dan (b) cryptosystem biometrik. Gambar-4 menunjukkan representasi grafis dari teknik perlindungan template biometric. Jenis lain dari teknik perlindungan template yang sedang air menandai [14], steganografi [15], sistem pada kartu / pertandingan pada kartu [2] dll

Sebuah. fitur Transformasi

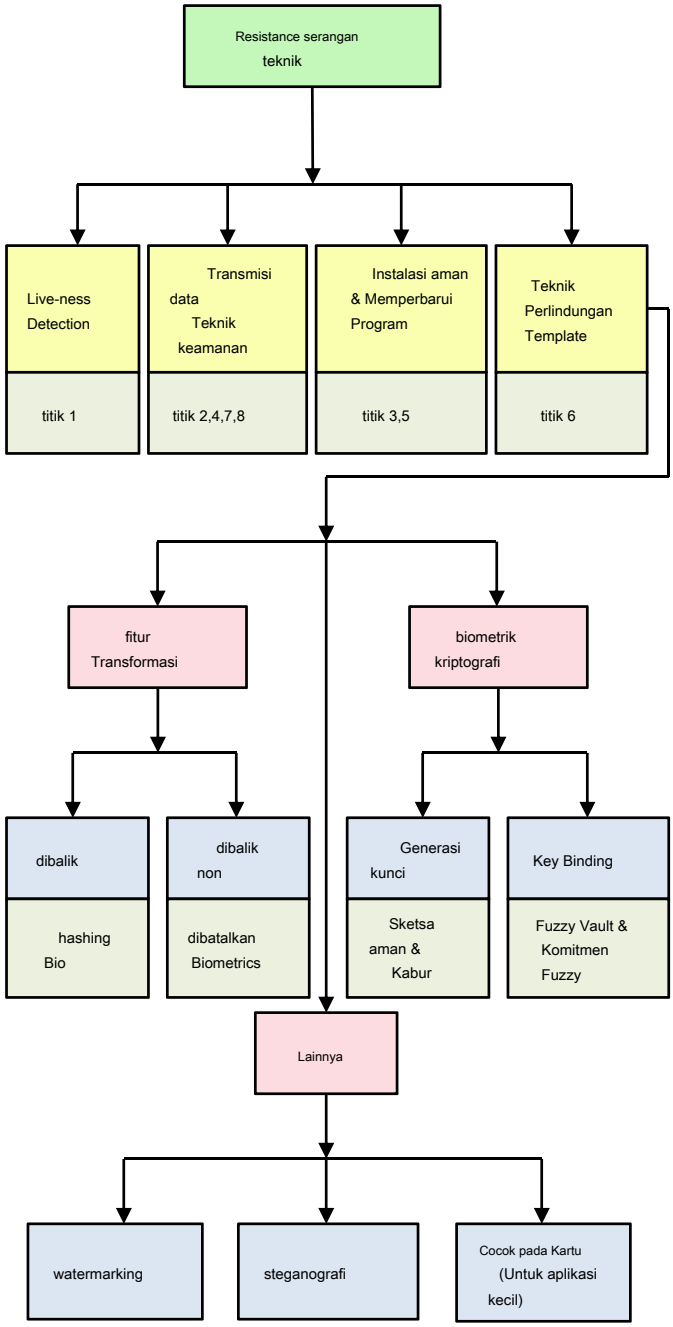
Untuk perlindungan, fitur yang dihasilkan dari gambar masukan ditransformasikan ke bentuk baru. Hal ini tidak disimpan secara real

https://sites.google.com/site/ijcsis/ ISSN 1947-5500

membentuk agak disimpan dalam bentuk berubah. Bentuk mengubah dihasilkan dapat dibalik atau non-dibalik.

1. Dibalik Transformasi (Bio Hashing)

Dalam transformasi fitur dibalik, template ditransformasikan dengan beberapa parameter pengguna. Di lokasi otentikasi, template terbalik lagi dengan parameter rahasia. Skema ini tidak dapat memberikan keamanan yang tinggi tanpa



Gambar 4. Serangan dan Solusi di Fingerprint Authentication Sistem.

rahasia transformasi. Karena jika rahasia key (parameter transformasi) dikompromikan dengan penipu, mereka dapat kembali template. Jadi, kuncinya harus diamankan cukup. [17]

2. Non-dibalik Transformasi (Cancellable Biometrik)

Skema biometrik dibatalkan adalah distorsi berulang yang disengaja dan sistematis data template biometric dengan tujuan melindungi bawah transformational- keamanan template biometric berbasis. Dalam situs verifikasi, citra query diubah dalam yang sama dengan cara yang, kemudian dibandingkan. Dalam konsep transformasi dapat dibatalkan, template berubah dapat dibatalkan dan kembali mengeluarkan dengan mengubah parameter transformasi jika masalah dikeluarkan [9].

b. biometrik kriptografi

teknik kriptografi data biometrik disebut kriptografi biometrik di mana kunci (atau tombol) digunakan untuk mengenkripsi data biometrik. Kuncinya dapat dihasilkan dari data biometrik itu sendiri atau dari data eksternal. Pada matcher, kuncinya digunakan untuk mendekripsi data biometrik. mengamati itu literatur, kita membagi Biometric Kriptografi menjadi dua bagian besar: Generasi Key atau Key Binding.

1. Generasi Key

Pada saat pendaftaran, kunci unik dipilih dari fitur diekstrak dari sidik jari. Kunci ini tidak disimpan dalam database [10].

SEBUAH *aman Sketch* andal mereproduksi rahasia biometrik tanpa membocorkan informasi apapun. Ia bekerja dalam dua tahap: Generasi & Rekonstruksi. Dibutuhkan data biometrik sebagai masukan dan menciptakan sketsa data itu. Kemudian, di rekonstruksi, yang dihasilkan sketsa dan data cukup mirip (image query) dengan aslinya input data yang diberikan. Kemudian, mereproduksi data input asli. Dengan demikian, dapat digunakan untuk masukan biometrik rawan kesalahan andal mereproduksi tanpa menimbulkan risiko keamanan yang melekat dalam menyimpan mereka [11].

Extractor Fuzzy andal ekstrak hampir seragam keacakan R dari input. Hal ini kesalahan-toleran karena jika kita mengubah memberikan template yang berbeda dari jari yang sama, R tidak akan berubah. Resultan R hampir mirip dengan aslinya R. ini R digunakan sebagai kunci dalam aplikasi kriptografi [9].

2. Key Binding

Dalam kunci mengikat, kunci kriptografi terikat erat dengan template biometric sehingga tidak bisa dilepaskan tanpa otentikasi biometrik sukses dan tanpa mengakses template yang langsung [12]. Kuncinya Binding dapat dikategorikan sebagai Fuzzy Vault dan Komitmen Fuzzy.

Fuzzy Vault pertama kali diperkenalkan oleh Juels dan Sudan [13] sebagai konstruksi kriptografi. Ada digunakan dua set poin: poin disortir kabur dan poin sekam. The disortir

https://sites.google.com/site/ijcsis/ ISSN 1947-5500

kumpulan data diambil dari data biometrik. Meenakshi [11] menjelaskan kubah kabur dengan sistem biometrik. Dalam kerangka kubah fuzzy, kunci rahasia S dikunci oleh G, di mana G adalah unordered set dari sampel biometrik. Sebuah P polinomial dibangun dengan pengkodean rahasia S. polinomial ini dievaluasi oleh semua elemen dari himpunan unordered G. Sebuah kubah V dibangun oleh persatuan set unordered G dan titik sekam set C yang tidak di G. kubah The , V = GU C. persatuan set menyembunyikan titik sekam asli set point dari penyerang. Menyembunyikan set point asli mengamankan data rahasia S dan user biometrik Template T. kubah ini dibuka dengan template kueri T'. T 'diwakili oleh set unordered lain U'. Pengguna harus memisahkan sejumlah titik dari lemari besi V dengan membandingkan U' dengan V. Dengan menggunakan metode koreksi kesalahan, P polinomial dapat berhasil direkonstruksi jika tumpang tindih U' dengan U dan rahasia S akan diterjemahkan. Jika tidak ada tumpang tindih substansial antara U dan U' kunci rahasia S tidak diterjemahkan. membangun ini disebut kabur karena lemari besi akan mendapatkan diterjemahkan bahkan untuk nilai sangat dekat dari U dan U' dan kunci rahasia S dapat diambil. Oleh karena itu kabur lemari besi konstruksi menjadi lebih tepat untuk data biometrik yang memiliki ketidakjelasan melekat.

SEBUAH *Komitmen Fuzzy* Skema adalah salah satu di mana kunci seragam acak dengan panjang 1 bit (Binary vektor) yang dihasilkan dan digunakan untuk secara eksklusif indeks sebuah *nbit* codeword mengoreksi kesalahan kode yang sesuai di mana sketsa diekstrak dari template biometric disimpan dalam database [9].

G. Database-Matcher Saluran Serangan

Pada jenis serangan, template disimpan berasal dari database yang dimodifikasi sebelum mencapai ke matcher. Jadi, pencocok mendapat template dimodifikasi.

Mempertahankan transmisi data yang aman dapat memecahkan masalah. teknik deteksi kesalahan yang berbeda seperti cek paritas, checksum, CRC dapat digunakan untuk mengidentifikasi template ditransmisikan dimodifikasi atau tidak. [18]

H. Override Keputusan Akhir

Hasil akhir yang berasal dari matcher tersebut dimodifikasi oleh penipu. Ini mengubah keputusan asli (menerima / menolak) dengan mengubah skor pertandingan.

Mengirim hasilnya melalui saluran terpercaya dan menggunakan pengiriman aman dapat digunakan untuk mendapatkan hasil yang benar.

AKU AKU AKU. C ONCLUSION

Penelitian ini menyampaikan analisis menonjol pada kerentanan Fingerprint Authentication System dari setiap titik dari model dan menunjukkan sistem keamanan yang efektif yang ada sekarang. Karya ini membawa kerentanan dan surat berharga, dipadatkan bersama-sama, sistem otentikasi sidik jari. Berbagai jenis serangan seperti biometrik palsu, data yang replay, disintesis set fitur dan template database telah menjelaskan tentang bagaimana mereka terjadi. Makalah ini juga berisi itu pencegahan teknik melawan itu sesuai serangan. Sebagai database template bagian yang sangat sensitif dari sistem, teknik perlindungan yang telah dianalisis dengan signifikansi yang tinggi. Makalah ini bahkan menunjukkan upaya yang sangat kecil diambil seperti pertandingan pada kartu untuk keamanan template sidik jari. Dalam analisis, telah belajar bahwa serangan pada template sangat parah. Jika template terganggu, keamanan pemiliknya akan dilanggar. Jadi, keamanan template yang membutuhkan perhatian lebih dari otoritas penelitian. Meskipun beberapa jenis pekerjaan yang telah dilakukan pada keamanan template yang, mereka tidak mampu untuk memenuhi semua persyaratan seperti pemulihan, keamanan, privasi, akurasi pencocokan tinggi dll Jadi, pekerjaan kami berikutnya adalah untuk menghasilkan skema keamanan template yang efisien.

R EFERENCES

[1] Ratha, Nalini K., Jonathan H. Connell, dan Ruud M. Bolle. "Sebuah analisis hal kecil kekuatan yang cocok."Konferensi Internasional tentang Audio-Video dan Berbasis Biometrik Orang Authentication. Springer Berlin Heidelberg, 2001. [2] Jain, Anil K., Karthik Nandakumar, dan Abhishek Nagar. "Biometric keamanan template "Journal EURASIP tentang Kemajuan Signal Processing 2008 (2008):. 113. [3] T. Putte dan J. Keuning, "pengenalan sidik jari biometrik: tidak mendapatkan jari-jari Anda terbakar", Proc. IFIP TC8 / WG8.8, Conf Kerja Keempat. Smart Card Penelitian dan Adv. App., Hlm. 289-303, 2000. [4] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino. "Dampak buatan 'bergetah' jari pada sistem sidik jari." Proc. SPIE 4677, Optical Keamanan dan Palsu Pencegahan Teknik IV, April 2002. [5] Rogmann, Nils, dan Maximilian Krieg. "Liveness Deteksi di Biometrics."Biometrics Khusus Interest Group (BIOSIG), Konferensi internasional. IEEE 2015. [6] Uludag, Umut, dan Anil K. Jain. "Serangan pada sistem biometrik: a studi kasus di sidik jari."Proceedings of SPIE. Vol. 5306. 2004. [7] "Sidik Jari Biometrik: Alamat Privasi Sebelum Deployment." https://www.ipc.on.ca/wp-content/uploads/2008/11/fingerprint- Biosys-priv.pdf, 2008. [8] Cappelli, Raffaele, Dario Maio, Alessandra Lumini, dan Davide Maltoni. "Gambar rekonstruksi sidik jari dari template standar." Transaksi IEEE pada analisis pola dan mesin kecerdasan 29, No.9. 2007. [9] Mwema, Joseph, S. Kimani, dan M. Kimwele. "Sederhana Ulasan Skema biometrik Template Perlindungan Digunakan di Mencegah Serangan Musuh di biometrik sidik jari Template "International Journal of Tren Komputer dan Teknologi 20,1 (2015):. 12-18. [10] Khandelwal, Sarika, PC Gupta, dan Khushboo Mantri. "Survei Ancaman terhadap Sistem Otentikasi Biometrik dan Solusi."International Journal of Aplikasi Komputer 61,17. 2013. [11] Meenakshi VS, "Aman Dan dibatalkan Biometric Template Menggunakan Fuzzy Vault Untuk Sidik Jari, Iris Dan Retina "A Thesis Dikirim Untuk Avinashilingam Dianggap Universitas Untuk Wanita Coimbatore. - 641.043 2010.

[12] Huixian, Li, et al. "Key mengikat berdasarkan perisai biometrik fungsi."Informasi Assurance dan Keamanan. IAS'09. Kelima Konferensi Internasional. Vol.1. IEEE 2009. [13] Juels, Ari, dan Madhu Sudan. "Skema kubah kabur." Designs, Kode dan Kriptografi 38,2 (2006): 237-257. [14] Patel, Monika, dan Priti Srinivas Sajja. "Dampak signifikan dari Biometrik Watermark untuk Memberikan Gambar Keamanan menggunakan berdasarkan DWT Alpha Blending Watermarking Teknik."[15] Rubal Jain dan Chander Kant. "Serangan terhadap Sistem Biometrik: Sebuah Ikhtisar "International Journal of Kemajuan dalam Penelitian Ilmiah 2015.; 1 (07): 283-288.

[16] M. Villa dan A. Verma. "Fingerprint Recognition," di Biometrics di Dunia Data Driven:.. Tren, Teknologi, dan Tantangan, M. Gofman dan S. Mitra Eds, CRC Press, USA, pp 265-281, 2017.

[17] Ramu, T., dan T. Arivoli. "Biometric Template Security: Sebuah Overview." Prosiding Konferensi Internasional tentang Electronics. Vol. 65. 2012. [18] Siwach, Ajay, Sunil Malhotra, dan Ravi Shankar. "Analisis dari Skema Kesalahan Deteksi yang berbeda selama OFDM Signal." International Journal of Engineering Tren dan Teknologi-Volume4 Issue4- 2013

PENULIS PROFIL

Tanjarul Islam Mishu menerima gelar B.Sc. (Engg.) Di bidang Ilmu Komputer dan Teknik dari Jatiya Kabi Kazi Nazrul Islam University, Mymensingh, Bangladesh pada tahun 2016. Saat ini, dia mahasiswa di M.Sc. lembaga ini. bunga penelitiannya difokuskan pada Biometrics Sistem, Pengenalan Pola, Gambar Pengolahan, dan Data Mining.

Dr Md. Mijanur Rahman adalah anggota fakultas dari Departemen Ilmu Komputer dan Teknik, Jatiya Kabi Kazi Nazrul Islam University, Trishal, Mymensingh, Bangladesh, sejak April 2008 (sangat awal universitas). Sekarang, Dr. Rahman bekerja sebagai Associate Professor CSE departemen. Dia juga menjabat sebagai Dosen dan Asisten Profesor di departemen yang sama. Ia menjabat sebelum sebagai Pengajar (Tech) Komputer di Pemerintah. Polytechnic Institute dari Desember 2005 hingga April 2008. Dr. Rahman memperoleh gelar B. Sc. (Hons) dan M. Sc. Gelar kedua dengan kelas pertama dalam CSE dari Universitas Islam, Kushtia, Bangladesh. Dia juga memperoleh gelar PhD di bidang Ilmu Komputer dan Teknik dari Universitas Jahangirnagar, Savar, Dhaka, Bangladesh pada bulan Agustus 2014. pengajaran dan bunga Penelitiannya terletak pada bidang-bidang seperti Digital Signal Processing, Digital Speech Processing, Biometric Technology, Pengenalan Pola, dll . Banyak dari makalah penelitiannya telah dipublikasikan di kedua jurnal nasional dan internasional.

https://sites.google.com/site/ijcsis/ ISSN 1947-5500