ANALISA KEAMANAN DATA SIDIK JARI PADA SMARTPHONE

Nyoman Ayu Nila Dewi[1)], I Nyoman Yudi Anggara Wijaya[2)]
Program Studi Sistem Informasi[1),2)]
Institut Teknologi dan Bisnis STIKOM Bali[1)], STMIK Primakara[2)]
nilaayudewi@gmail.com[1)], inyomanyudi@gmail.com[2)]

ABSTRACT

The development of smartphones as a communication tool and also the dissemination of information is very rapid, by using only smartphones, people can communicate, store data such as photos, and can also directly carry out banking transactions through these devices. Smartphones are considered a primary need for communicating and storing data. Personal data that really helps the community with the convenience of a smartphone is also offset by the danger that threatens the security of the data stored on the device. Biometric identification techniques, based on physiological characteristics, such as facial characteristics, fingerprints, irises, DNA, palms and behavioral characteristics, such as signature and voice. The development of security technology using biometrics has been widely used, especially by using fingerprints. Behind the security that is considered better and the ease with which the fingerprint system has, does the security system have a loophole to be dismantled. Security for locking smartphone devices using fingerprints is a computing model that has various advantages. But behind that, the security of information about fingerprints and data contained in the device is important.
Keywords: *Data Security, Fingerprint*

ABSTRAK

Perkembangan smartphone sebagai alat komunikasi dan juga penyebaran informasi sangat pesat, dengan hanya menggunakan smartphone masyarakat sudah dapat berkomunikasi, menyimpat data-data seperti foto, dan juga sudah dapat langsung berteransaksi perbankan melalui perangkat tersebut Smartphone yang sudah dianggap sebagai kebutuhan primer untuk berkomukasi dan menyimpan data-data pribadi yang sangat membantu masyarakat dengan kemudahannya yang dimiliki smartphone juga diimbangi dengan bahanya yang mengamcam keamanan data-data yang disimpan di dalam perangkat tersebut. Teknik identifikasi secara biometrik, didasarkan pada karakteristik fisiologis, seperti karakteristik wajah, sidik jari, iris mata, DNA, telapak tangan dan karakterisitik perilaku, seperti tanda tangan dan suara. Perkembangan teknologi keamanan dengan menggunakan biometric sudah banyak digunakan khususnya dengan menggunakan sidik jari. Dibalik keamanan yang dianggap lebih baik dan kemudahan yang dimiliki sistem sidik jari apakah sistem keamanan tersebut memiliki celah untuk dibongkar. Keamanan untuk penguncian perangkat smartphone dengan menggunakan sidik jari merupakan model komputasi yang memiliki beragam keuntungan. Namun dibalik itu, keamanan terhadap informasi mengenai sidik jari dan data yang terdapat di dalam perangkat tersebut merupakan hal penting.
Kata Kunci : Keamanan Data, Sidik Jari

PENDAHULUAN

Kebutuhan masyarakat pada masa ini akan informasi sangat terlihat dari prilaku masyarakat yang selalu mencari keterbaruan informasi. Perkembangan teknologi komunikasi dan informasi menggeser penyebaran informasi dengan media konvensional seperti koran, majalah dan televise. Teknologi telekomunikasi dan informasi memudahkan penyebaran informasi yang langsung sampai ketangan masyarakat dengan menggunakan smartphone, tablet ataupun personal computer.

Seiiring perkembangan teknologi informasi untuk penyebaran informasi, perkembangan keamanan terhadap informasi tersebut juga harus diperhatikan. Salah satu keamanan informasi yang umum digunakan dan banyak digunakan untuk melindungi data yang terdapat dalam personal komputer adalah antivirus, antivirus digunakan untuk melindungi data dan informasi masi dari manipulasi (Pratiwi 2011).

Perkembangan smartphone sebagai alat komunikasi dan juga penyebaran informasi sangat pesat, dengan hanya menggunakan smartphone masyarakat sudah dapat berkomunikasi, menyimpat data-data seperti foto, dan juga sudah dapat langsung berteransaksi perbankan melalui perangkat tersebut (Pratiwi 2011). Smartphone yang sudah dianggap sebagai kebutuhan primer untuk berkomukasi dan menyimpan data-data pribadi yang sangat membantu masyarakat dengan kemudahannya yang dimiliki smartphone juga diimbangi dengan bahanya yang mengamcam keamanan data-data yang disimpan di dalam perangkat tersebut.

Teknik konvensional yang sering digunakan untuk keamanan perangkat smartphone adalah menggunakan *password.* Akan tetapi, teknik di atas ternyata tidak cukup efektif, karena sangat mudah untuk diketahui oleh pihak yang tidak berwenang. Untuk mengatasi masalah di atas, dikembangkanlah suatu metode identifikasi secara biometrik. Teknik identifikasi secara biometrik, didasarkan pada karakteristik fisiologis, seperti karakteristik wajah, sidik jari, iris mata, DNA, telapak tangan dan karakterisitik perilaku, seperti tanda tangan dan suara (Gazali et al. 2012). Perkembangan teknologi keamanan dengan menggunakan biometric sudah banyak digunakan khususnya dengan menggunakan sidik jari.

Banyak semartphone yang beredar dipasaran sudah menggunakan teknik keamanan sidik jari untuk mengmankan smarphone tersebut, keamanan sidik jari di anggap lebih aman dan efektif karena karakteristik secara biometrik tidak mudah untuk dicuri oleh pihak-pihak yang tidak berwenang (Gazali et al. 2012). Dibalik keamanan yang dianggap lebih baik dan kemudahan yang dimiliki sistem sidik jari apakah sistem keamanan tersebut memiliki celah untuk dibongkar.

IDENTIFIKASI MASALAH

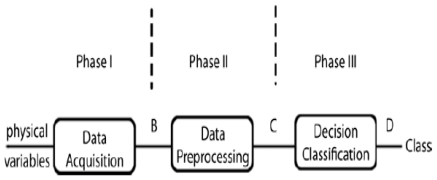
Penggunaan keamanan sidik jari pada smartphone sudah umum digunakan namun bagaimana pembuat semartphone tersebut dapat mempertanggujawabkan keamanan data sidik jari pengguna handphone tersebut dan bagaimana tingkat keamanan scanner sidik jari pada perangkat handphone tersebut.

MEMBACA POLA

Saat ini telah berkembang sistem kecerdasan buatan yang ditanamkan pada perangkat komputer maupun perangkat semartphone . Dengan berkembangan sistem kecerdasan buatan komputer dapat mengenali secara visual seperti mengenali sebuah obyek. Untuk dapat melakukan hal tersebut sistem harus melakukan pengelohan citra agar gambar yang ditangkap oleh komputer atau perangkat semartphone jelas, setelah gambar yang dihasilkan jelas, selanjutnya komputer melakukan pengenalan pola untuk mengenali citra tersebut (Sweetania 2012).

Tahapan untuk melakukan pengenalan pola dibagi menjadi tiga tahap, yaitu :

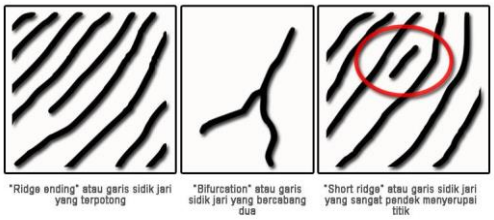
1. *data acquisition* yaitu tahapan saat data analog akan rekam pada perangkat penerjemah yang akan membuatnya data analog tersebut menjadi data digital yang dapat diolah oleh komputer.
2. *data preprocessing* yaitu tahap saat data digital yang diperoleh dari tahap data acquisition diekstraksi karakteristiknya dan kemudian karakteristik tersebut menjadi data *output*.
3. *decision classification* yaitu tahap saat karakteristik yang diperoleh pada tahap sebelumnya, digunakan untuk mengklasifikasikan obyek.



Gambar 1. 1Alur Proses Pemindaian Sidik Jari (Gazali et al. 2012)

SIDIK JARI

Sidik jari merupakan identitas unik yang dimiliki oleh setiap manusia, hal ini membuat sidik jari seringkali digunakan dalam teknologi biometrik. Keunggulan lain dari sidik jari adalah kepraktisannya dan ketahanannya. Suatu pola sidik jari terdiri dari beberapa garis seperti ujung garis (*ridge ending*), garis bercabang (*bifurcation*), dan garis pendek menyerupai titik (*short ridge*) (Putri 2016). Tiga detail pada sidik jari ini tak pernah ditemui sama pada manusia.



HASIL DAN PEEMBAHASAN

Data sidik jari pada manusia sangat penting, hal ini dikarenakan sidik jari sering kali digunakan sebagai sistem pengamanan atau pengenalan tersehadap seseorang. Sidik jari yang direkam oleh smartphone dan selanjutnya dijadikan sebagai sistem pengeamanan perangkat tersebut apakah dapat dipertanggungjawabkan oleh pembuat perangkat tersebut.

Antisipasi Kekurangan Keamanan

Agar informasi yang terdapat pada smartphone dapat terjaga keaslian data dan keamanan informasinya terutama informasi sidik jari pengguna, maka perlu memperhatikan beberapa hal.

1. Perlu mengetahui bagaimana penyimpanan data sidik jari pada smartphone tersebut, apakah disimpan hanya pada local device atau disimpan pada cloud computing yang dimiliki perangkat tersebut.
2. Memastikan tersedianya perlindungan hak milik intelektual dan kerahasiaan atas data sidik jari yang kita simpan pada media penyimpanan cloud.
3. Pembacaan sidik jari sangat bergantung pada kondisi kulit telapak jari. Jika telapak jari kotor atau kulit sedang terkelupas, pembaca sidik jari bisa saja gagal mengenali pola dari sidik jari.
4. Kemungkinan dapat meniru sidik jari dan digunakan untuk membuka lock handphone Anda. Dengan cara menciptakan copy dari sidik jari menggunakan cartridge tinta khusus dan kertas. Tinta melakukan konduksi listrik pada kertas khusus ini, dan menciptakan cetakan sirkuit. Langkah berikutnya adalah untuk memindai sidik jari seseorang dalam resolusi tinggi dan mencetak dengan printer inkjet.

Penanganan Acaman Keamanan Data

1. Penyimpanan data sidik jari pada semartphone. Penggunaan smartphone dengan keamanan kunci sidik jari akan menyimpan informasi terhadap sidik jari pengguna, untuk menghidari penyebaran informasi mengenai sidik jari pengguna, sebaiknya pengguna melakukan penyimpanan sidik jari yang secara offline, dan untuk backup file pada smartphone dilakukan secara offline juga.
2. Memastikan bagaimana perangkat tersebut dapat menjamin kemamanan data yang disimpan pada cloud computing milik perangkat tersebut. Penyimpanan backup otomatis yang dilakukan oleh semartphone sangat jarang diperhatikan oleh pengguna smartphone. Penggunaan backup secara otomatis pada smartphone umumnya disimpan pada cloud computing milik perangkat tersebut. Hal penting yang harus dilakukan sebelum user menentukan *smartphone* adalah dengan memeriksa standar dan proses keamanan jaringan terhadap penyimpanan cloud yang mereka terapkan.
3. Pembacaan sidik jari saat telapak sidik jari rusak dan bagaimana agar alat untuk membaca sidik jari lebih sensitive. Untuk menangani kekurangan tersebut, smartphone sebaiknya menggunakan sensor ultrasonik atau kapasitans

(*capacitive*). Sensor ultrasonik, sesuai namanya, memanfaatkan gelombang ketika memindai sidik jari seperti pada ultrasonografi (USG) yang kerap digunakan untuk keperluan medis. Hasil pemindaian sidik jari dengan sensor tersebut sudah berkualitis tiga dimensi (3D) sehingga kemungkinan pemalsuan lebih rendah. Identifikasi menggunakan sensor ultrasonik juga tak bergantung pada kualitas kulit jari.

SIMPULAN

Keamanan untuk penguncian perangkat smartphone dengan menggunakan sidik jari merupakan model komputasi yang memiliki beragam keuntungan. Namun dibalik itu, keamanan terhadap informasi mengenai sidik jari dan data yang terdapat di dalam perangkat tersebut merupakan hal penting.

DAFTAR PUSTAKA

[1] Fathansyah, I., 2002. Basis Data. Bandung: Informatika.

[2] Sweetania, D., 2012. ANALISA ALGORITMA SISTEM KEAMANAN KOMPUTER MENGGUNAKAN SIDIK JARI DENGAN METODE POIN MINUTIAE PADA HP COMPACT 2210B NOTEBOOK PC. *UG Jurnal*, 6(01), pp.18–21

[3] Putri, A.A., 2016. Begini Cara Kerja Sensor Fingerprint pada Smartphone. Kompas Tekno. Diakses pada 07-12-2016

[4] Pratiwi, O.N., 2011. ANALISIS KEAMANAN APLIKASI PENYIMPANAN DATA PADA SISTEM CLOUD COMPUTING. *Konfrensi Teknologi Informasi dan Komunikasi untuk Indonesia*, pp.137–139

[5] Gazali, W., Agung, A. & Gunawan, S., 2012. ANALISIS DAN PEMBUATAN SISTEM PENGENALAN SIDIK JARI BERBASIS KOMPUTER DI POLDA METRO JAYA. *MAT STAT*, 12(9), pp.55–65

[6] Kadir, A., 2003. Pengenalan Teknologi Informasi. Yogyakarta: Andi Offset

[7] Maturidi, D. A., 2012. Metode Penelitian Teknik Informatika. Yogyakarta: Deepublish

[8] Rosa, A. & Shalauddin, M., 2013. Rekayasa Perangkat Lunak Terstruktur Dan Berorientasi Objek. Bandung: Informatika