Jurnal EurekaMatika

Journal homepage: https://ejournal.upi.edu/index.php/JEM

Autentikasi Dokumen Digital Pada *Cloud* Menggunakan Algoritma *Hashing* BLAKE2 dan *Rivert Shamir Adleman* (RSA)

*Sultan Maulana Akbar Djuandadesta, Rini Marwati, dan Dewi Rachmatin**

Program Studi Matematika, Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam
Universitas Pendidikan Indonesia
* Correspondence author: dewirachmatin@upi.edu

A B S T R A K

Pada era transformasi digital, menjaga keaslian dan integritas dokumen digital menjadi sangat penting, terutama saat disimpan dan diakses melalui *platform cloud*. Artikel ini menawarkan solusi kuat untuk autentikasi dokumen digital dengan menggabungkan fungsi *hash* BLAKE2 dan kriptografi RSA sebagai tanda tangan digital. BLAKE2 dikenal cepat dan aman dalam menghasilkan *hash* unik sebagai sidik jari digital setiap dokumen, sedangkan RSA berperan melindungi *hash* tersebut agar hanya pihak berwenang yang dapat memverifikasinya. Pendekatan ini mengintegrasikan *hashing* BLAKE2 dan enkripsi RSA dalam sistem *cloud* untuk membangun autentikasi dokumen yang aman dan efisien. Hasil penelitian menunjukkan metode ini mampu menjamin keamanan tinggi sekaligus mempertahankan kinerja optimal bagi organisasi dalam melindungi dokumen digital mereka.

INFORMASI ARTIKEL

Sejarah Artikel:

Diterima 16 Mar 2025
Direvisi 28 Oktober 2025
Disetujui 31 Oktober 2025
Tersedia online 2 Nopember 2025
Dipublikasikan 2 Nopember 2025

Kata Kunci:
BLAKE2,
Digital document authentication,
Digital signature algorithm,
RSA

A B S T R A C T

In the era of digital transformation, maintaining the authenticity and integrity of digital documents has become crucial, especially when they are stored and accessed through cloud platforms. This article presents a robust solution for digital document authentication by combining the BLAKE2 hash function and RSA cryptography as a digital signature algorithm. BLAKE2 is known for its speed and security in generating unique hashes that serve as digital fingerprints for each document, while RSA protects these hashes to ensure that only authorized parties can verify them. This approach integrates BLAKE2 hashing and RSA encryption within a cloud environment to establish a secure and efficient document authentication system. The findings indicate that this method ensures strong security while maintaining optimal performance for organizations in safeguarding their digital documents.

Keywords:
BLAKE2,
Digital document authentication,
Digital signature algorithm,
RSA.

1. PENDAHULUAN

Di abad ke-21 ini, perkembangan pesat terjadi terutama di bidang teknologi dan informasi. Inovasi dalam bidang ini telah melahirkan gagasan tentang *borderless world* di mana batas-batas geografis telah semakin kehilangan relevansinya. Konsep ini mencerminkan pandangan bahwa hambatan-hambatan terhadap pergerakan modal, teknologi, dan informasi akan semakin minim atau bahkan hilang sepenuhnya (Lakha & Taneja, 2009). Salah satu bentuk inovasi pada bidang teknologi dan informasi adalah *cloud computing*. informasi adalah komputasi awan atau *cloud computing***.** *Cloud computing* adalah penggunaan sumber daya komputasi (*hardware* dan *software*) yang dijadikan sebagai sebuah layanan melalui jaringan, seperti internet (Kacha & Zitouni, 2017). *Cloud computing* juga didefinisikan sebagai mekanisme yang memudahkan akses jaringan dan sesuai permintaan sebuah kumpulan perangkat seperti *server*, jaringan, perangkat penyimpanan, aplikasi, dan perangkat komputasi canggih lainnya (Paul & Ghose, 2012).

Cloud computing merupakan sebuah inovasi yang telah terintegrasi dan teradopsi secara masif oleh umat manusia. Salah satu contoh penggunaannya adalah pertukaran informasi menggunakan dokumen digital yang dibagikan melalui internet. Dokumen digital sering digunakan untuk menyimpan informasi sensitif yang kemudian dibagikan atau disebarluaskan. Akan tetapi, dokumen digital dapat dengan mudah dibaca dan diubah oleh pihak yang tidak bertanggung jawab sehingga rentan terhadap perubahan tidak sah. Oleh karena itu, diperlukan upaya perlindungan integritas dokumen dengan ilmu kriptografi yang dapat mencegah dokumen digital yang memiliki konten sensitif dari serangan siber, seperti serangan *Man in the Middle* (MitM) yang melibatkan pihak luar yang tidak disetujui memasuki jaringan dan mengubah informasi sensitif tanpa sepengetahuan pengguna (Andreeva *et al*., 2013).

Tanda tangan digital atau digital signature adalah sebuah metode yang memastikan sebuah plainteks dengan bentuk, seperti dokumen, teks, atau audio terjaga integritasnya dan mencegah perubahan yang tidak sah. Tanda tangan digital berbasis kriptografi kunci publik, seperti yang dikemukakan (Singh, 2015), dapat memberikan platform yang aman untuk pertukaran data, verifikasi integritas, dan pembuktian integritas pengirim. Tanda tangan digital merupakan sebuah metode untuk memastikan keaslian dan integritas dari dokumen digital. Tanda tangan digital dapat memberikan kepercayaan yang nyata dengan mencegah dan mendeteksi ketidaksesuaian atau kesalahan yang dapat mempengaruhi integritas informasi (Ferreira *et al*., 2004). Metode tanda tangan digital melibatkan proses enkripsi serta dekripsi, pembangkitan kunci publik dan privat dan tanda tangan menggunakan kriptografi kunci publik dan fungsi *hash*.

Fungsi *hash* kriptografi adalah algoritma keamanan penting yang digunakan dalam tanda tangan digital (Mouha *et al*., 2018). Fungsi *hash* BLAKE adalah fungsi *hash* kriptografi yang dibuat berdasarkan pada *stream cipher* ChaCha. BLAKE merupakan algoritma fungsi *hash* yang menjadi finalis pada NIST SHA-3 Cryptographic Hash Algorithm Competition pada tahun 2012 yang dirancang oleh tim ahli di bidang kriptanalis, implementasi, dan rekayasa kriptografi, yaitu Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, dan Christian Winnerlein. BLAKE2 merupakan versi yang ditingkatkan dari BLAKE yang dioptimalkan untuk perangkat lunak, BLAKE2 hadir dalam dua varian utama: BLAKE2b dioptimalkan untuk platform 64-bit, dan BLAKE2s untuk arsitektur yang lebih kecil dan salah satu target aplikasi dari BLAKE2 adalah penyimpanan awan atau *cloud storage* (Aumasson *et al*., 2013).

Dibandingkan fungsi *hash* lain yang ada saat ini, BLAKE2 lebih cepat daripada MD5 dan memberikan keamanan yang serupa dengan SHA-3 dengan *collision resistance* 256-bit dan memiliki kekebalan terhadap *length extension* (Aumasson *et al*., 2013). Didukung juga oleh analisis lain yang telah dilakukan, BLAKE2 memiliki keamanan yang sangat tinggi dari semua serangan yang telah diketahui (Guo *et al*., 2014), memiliki ketahanan terhadap serangan *bruto force* (Mallik, 2019), dan secara optimal aman terhadap *collision, preimage,* dan *second image* (Andreeva *et al*., 2013).

Kriptografi RSA (Rivest-Shamir-Adleman) merupakan sebuah kriptografi kunci publik yang ditemukan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman yang diperkenalkan pada tahun 1977. Kriptografi RSA terdiri atas tiga proses yaitu pembangkitan kunci, enkripsi dan dekripsi dan karena algoritma ini termasuk algoritma asimetris maka pada proses pembangkitan kunci dibangkitkan dua kunci, yaitu kunci publik (n, e) dan kunci rahasia (d) oleh penerima pesan (Firdaus *et al.*, 2018) dan sistem kriptografi RSA masih merupakan keamanan yang baik untuk mengirimkan data sensitif (Berlin & Dhenakaran, 2017).

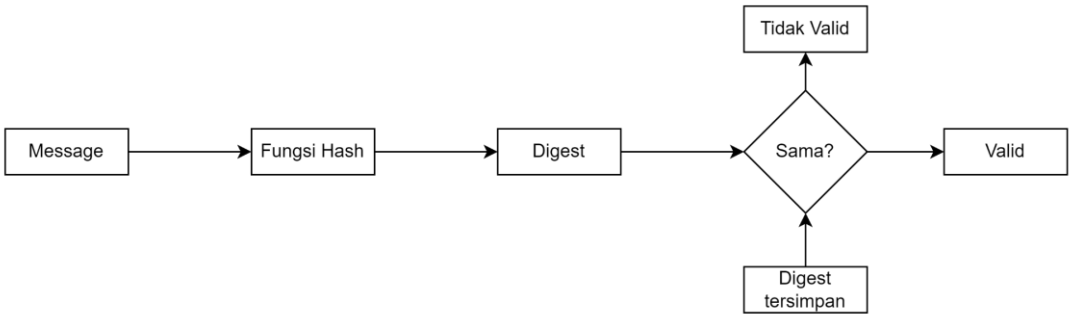
Dalam konteks keterbaruan dari penelitian ini, inovasi terkait implementasi BLAKE2 yang dikombinasikan dengan RSA pada *cloud* menjadi aspek utama yang mencerminkan tuntutan terhadap era teknologi informasi yang terus berkembang. Implementasi BLAKE2 yang dikombinasikan dengan RSA pada *cloud* menciptakan dimensi baru dalam pemrosesan dan penyimpanan dokumen digital dengan menitikberatkan pada kecepatan, efisiensi, dan keamanan. Penelitian yang telah dilakukan melibatkan aplikasi konkret dan konsep-konsep kriptografi ke dalam kehidupan sehari-hari, khususnya dalam konteks *cloud computing* yang menjadi media utama penyimpanan dan pertukaran data masa kini. Oleh karena itu diharapkan dari hasil penelitian ini dapat memberikan manfaat teoritis dan praktis terhadap pengamanan dokumen-dokumen digital dan keberlanjutan penggunaannya dalam konteks teknologi informasi modern.

Dokumen digital cenderung memiliki karakteristik terbuka atau dapat diakses oleh pihak yang memiliki izin, yang membuatnya rentan terhadap data *tampering* atau modifikasi yang tidak sah selama proses transfer atau penyimpanan. Data *tampering* atau modifikasi yang tidak sah terhadap data akan menyebabkan kekhawatiran akan keaslian dokumen, kurangnya kepercayaan, risiko keamanan, dan masih banyak lagi. Oleh karena itu, untuk melindungi dokumen digital berformat .pdf yang disimpan atau dibagikan melalui layanan *cloud* dari berbagai jenis serangan siber yang dapat merusak integritas dokumen, diperlukan tindakan perlindungan, seperti penggunaan tanda tangan digital. Tanda tangan digital atau *digital signature* merupakan sebuah metode untuk mengecek keautentikan atau keaslian sebuah dokumen digital berformat .pdf. Dengan mengecek *signature* yang tertanam dalam dokumen digital dapat diverifikasi apakah telah terjadi perubahan terhadap dokumen digital atau tanda tangan yang tertanam pada dokumen tersebut.

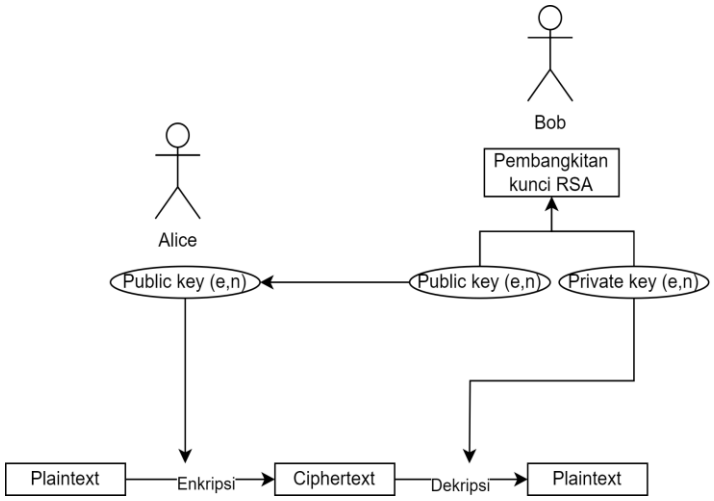
Model Dasar

Penelitian ini menggunakan model dasar berupa fungsi *hash* dan algoritma tanda tangan RSA. Algoritma tanda tangan digital RSA merupakan algoritma kunci asimetris yang memanfaatkan kunci privat untuk pembuatan tanda tangan dan kunci publik untuk verifikasinya. Proses penandatanganan dan verifikasi menggunakan nilai hash yang dihasilkan dari fungsi hash BLAKE2. Pada penelitian ini, input yang digunakan adalah *file* berformat PDF, yang merupakan format umum untuk menyimpan data sensitif dan salah satu format paling umum untuk file yang disebarluaskan.

Perhatikan Gambar1, algoritma tanda-tangan digital RSA bekerja dengan menggunakan sepasang kunci, yaitu kunci publik dan kunci privat. Selanjutnya pada Gambar 2, proses tanda tangan digital RSA melibatkan penggunaan kunci privat untuk menghasilkan tanda tangan digital, yang nantinya dapat diverifikasi oleh pihak lain menggunakan kunci publik yang sesuai.



Gambar 1. Skema Fungsi Hash Sebagai Tanda-tangan

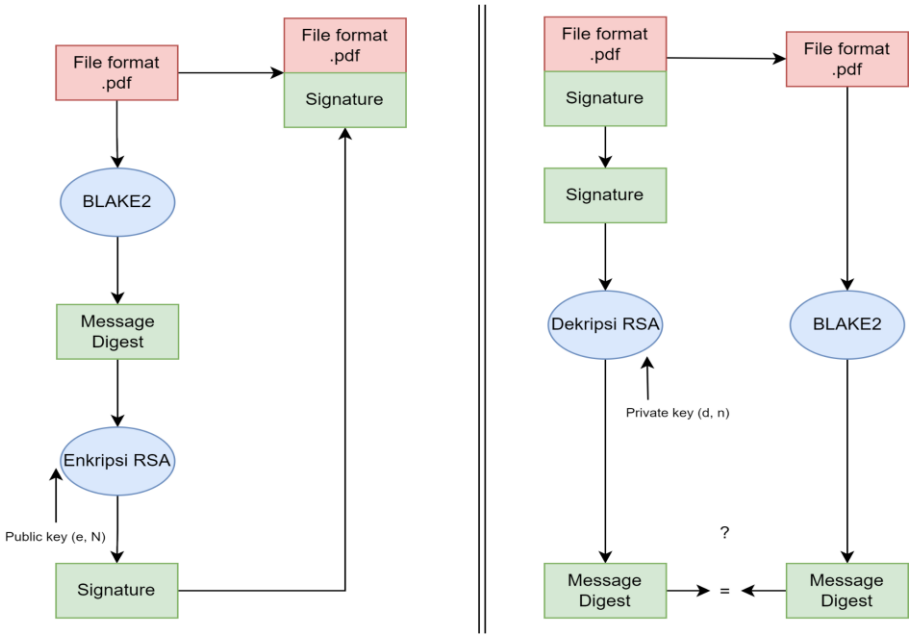


Gambar 2. Skema Kriptografi RSA

Pengembangan Model

Berdasarkan model dasar yang telah dijelaskan sebelumnya, pengembangan dalam penelitian ini dilakukan dengan mengimplementasikan fungsi *hash* BLAKE2 dalam skema tanda-tangan RSA. Ini akan menghasilkan nilai *hash* sebesar 512-bit di lingkungan *cloud*.

Pada Gambar 3, cara kerja aplikasi yang akan dibuat, dimulai dari pengguna yang mengunggah *file* berformat .pdf. *File* tersebut kemudian akan diproses dengan fungsi *hash* BLAKE2 untuk menghasilkan *message digest* yang dienkripsi menggunakan algoritma RSA, menghasilkan *signature* yang akan ditambahkan ke *file* .pdf yang diunggah oleh pengguna.



Gambar 3. Skema pengembangan model

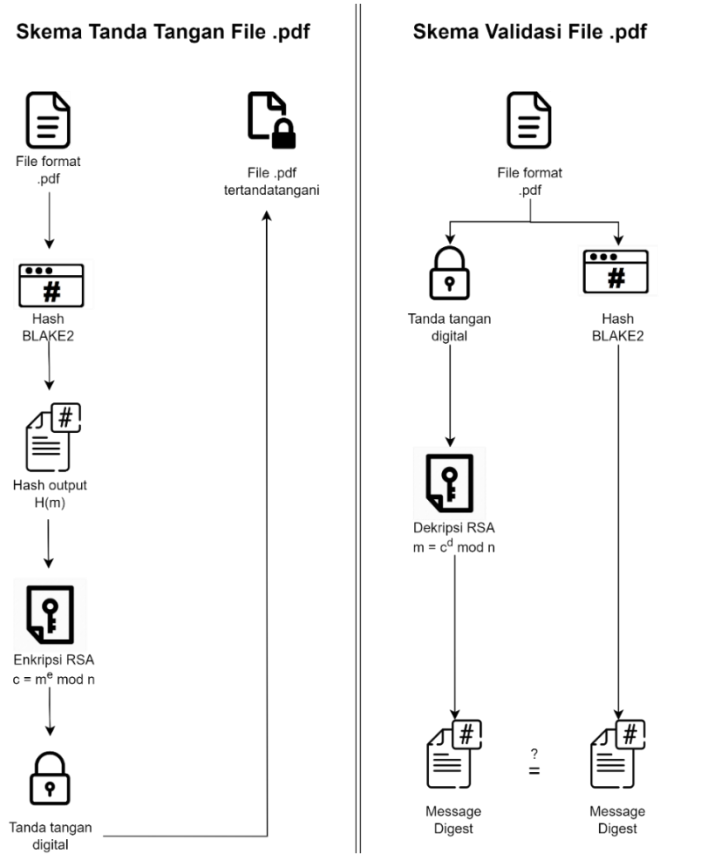
Proses validasi integritas *file* dilakukan ketika pengguna mengunggah *file* .pdf yang akan didekripsi oleh aplikasi. Secara bersamaan, *file* tersebut akan di-*hash* untuk mendapatkan *message digest. Message digest* hasil dekripsi kemudian dibandingkan dengan *message digest* hasil *hashing*. Jika nilainya sama, maka integritas *file* tersebut telah tervalidasi dengan benar, dan jika tidak, maka integritas *file* tidak valid.

3. Hasil dan Pembahasan

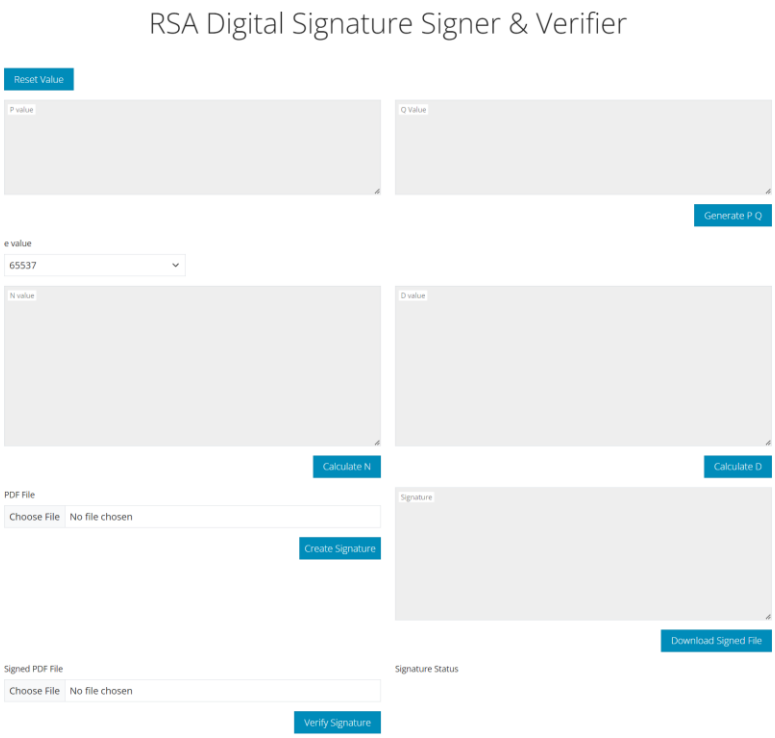
Skema implementasi penggabungan algoritma Kripgtografi RSA dan fungsi *hash* BLAKE2 pada Aplikasi Tanda-tangan Digital Dengan RSA & BLAKE2 dapat dilihat pada Gambar 4. Aplikasi berbentuk *webapp* atau aplikasi berbasis web dan dibuat berdasarkan algoritma dan skema yang telah dipaparkan seperti pada Gambar 5. Aplikasi tersebut dibuat dengan bahasa pemrograman Python versi 3.11.6 pada komputer dengan spesifikasi Windows 11 64-bit, *processor* Intel Core i5-8250U dan RAM 8 GB.

Setelah program aplikasi telah selesai dikonstruksi, dilakukan proses validasi dengan melakukan pengecekan terhadap keluaran dari aplikasi yang telah dibuat untuk melihat apakah aplikasi berjalan sesuai fungsinya atau tidak. Validasi dilakukan dengan dua buah jenis kasus, yaitu:

1. Verifikasi dokumen digital yang autentik dengan terdapatnya kesesuaian tanda tangan digital yang diunggah
2. Verifikasi dokumen digital yang tidak autentik dan terdapat perubahan pada tanda tangan digital yang tertanam.



Gambar 4. Skema Aplikasi Tanda Tangan Digital Dengan RSA & BLAKE2



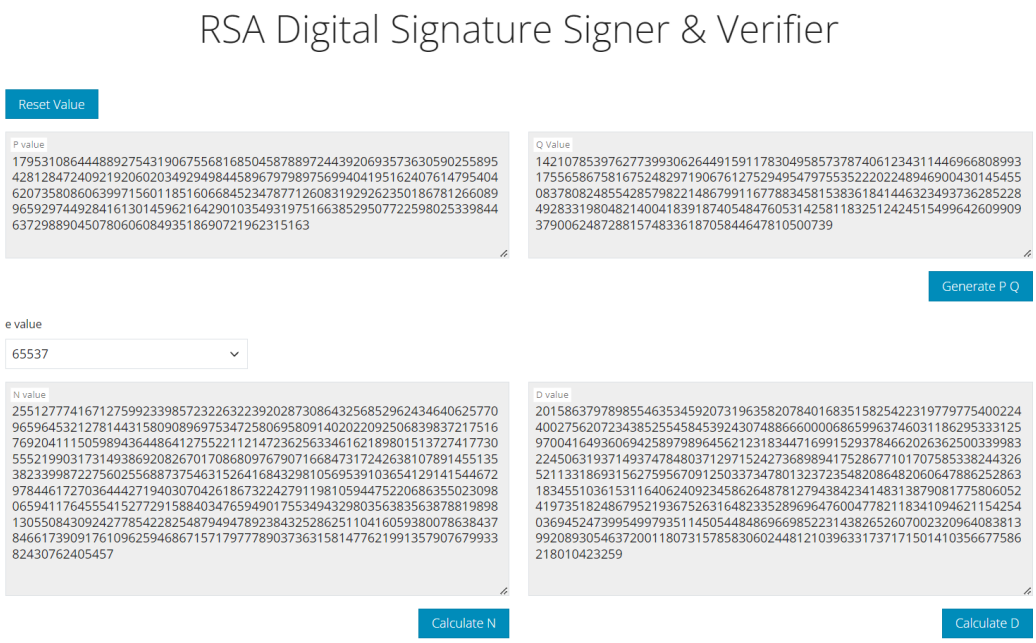
Gambar 5. Tampilan Aplikasi Tanda Tangan Digital Dengan RSA & BLAKE2

Kasus Pertama

Pada kasus pertama ini, akan dilakukan validasi terhadap sebuah dokumen digital berupa slip gaji yang merupakan dokumen digital bersifat sensitif. Berikut adalah tahapan dalam proses validasi dokumen digital tersebut:

1. **Pembangkitan kunci RSA**

Perhatikan Gambar 6, setelah dibangkitkannya kunci pada aplikasi tanda tangan digital, didapatkan dua pasang kunci publik dan kunci privat, yaitu:



Gambar 6. Pembangkitan Kunci Untuk Validasi Kasus Pertama

- Kunci publik (e,n): (65537,
25512777416712759923398572322632239202873086432568529624346406257709659645321278144315809089697534725806958091402022092506839837217516776920411150598943644864127552211214723625633461621898015137274177305552199031731493869208267017086809767907166847317242638107891455135382339987227560255688737546315264168432981056953910365412914154467297844617270364442719403070426186732242791198105944752206863550230980659411764555415277291588403476594901755349432980356383563878819898130550843092427785422825487949478923843252862511041605938007863843784661739091761096259468671571797778903736315814776219913579076799338243076240545 7)
- Kunci privat (d,n):
(20158637978985546353459207319635820784016835158254223197797754002244002756207234385255458453924307488666000068659963746031186295333125970041649360694258979896456212318344716991529378466202636250033998322450631937149374784803712971524273689894175286771017075853382443265211331869315627595670912503373478013237235482086482060647886252863183455103615311640624092345862648781279438423414831387908177580605241973518248

67952193675263164823352896964760047782118341094621154254036945247399549979351145054484869669852231438265260700232096408381399208930546372001180731578583060244812103963317371715014103566775862180104232592551277741671275992339857232263223920287308643256852962434640625770965964532127814431580908969753472580695809140202209250683983721751676920411150598943644864127552211214723625633461621898015137274177305552199031731493869208267017086809767907166847317242638107891455135382339987227560255688737546315264168432981056953910365412914154467297844617270364442719403070426186732242791198105944752206863550230980659411764555415277291588403476594901755349432980356383563878819898130550843092427785422825487949478923843252862511041605938007863843784661739091761096259468671571797778903736315814776219913579076799338243076240545 7).

2. Tanda tangan dokumen slip gaji

Selanjutnya, akan diunggah dokumen digital slip gaji untuk dapat dibuat tanda-tangan digitalnya untuk ditanam pada dokumen slip gaji tersebut seperti pada Gambar 7.

Gambar 7. Pembuatan Tanda-tangan Untuk Validasi Kasus Pertama

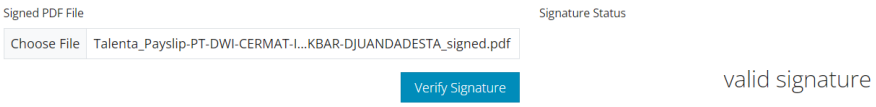
Dengan mengunggah dokumen slip gaji tersebut dan dengan fungsi *hash* BLAKE2 kita mendapatkan sebuah tanda tangan digital dengan nilai:
569f6bfb28523f4d0155c9f9041a7a3ce4d2d4f3ba8b3d9f659d45af907eb804187b60ae17e5691a957215112597914fb5ab9b228f6af3fa814b41127e3b08212459ddd0aa63c929e09086decac8db65c12f2a050085e333b55c1e619b44724fe35bd2697e1628cf790162f1b062ce128d79c709fe3a50afd5686cfd493836d3608c2cb7b379257ec8726df498e8cbda04ea6908a0b460c7084c5d25cc92942c8bf2288cdc4d2fc883c3fa07e890f8b13e5427fd4e0829de87706a61951ea3b7a205a499e22c5e3732d0fb573d6d26a93478b9cfd937d3f1f2cef7470fb73598580862f60d7e401224da3b8fb212933883a15da5beca56502192188ee533cac0.

Selanjutnya setelah diunduh dokumen digital yang telah tertandatangani dan membukanya pada *text editor* kita dapat melihat bahwa tanda tangan tersebut telah tersematkan pada dokumen slip gaji seperti pada Gambar8.

Gambar 8. Tanda-tangan Digital Tersematkan Pada Dokumen Slip Gaji

3. Validasi tanda tangan digital pada dokumen slip gaji

Untuk memvalidasi apakah dokumen digital slip gaji tersebut masih terjaga integritasnya setelah dikirim atau dibagikan sesuai dengan keperluan pengguna, maka diunggah kembali dokumen slip gaji yang sudah tertandatangi tersebut pada aplikasi dan menekan *button* 'Verify Signature' seperti pada Gambar 9.



Gambar 9. Validasi Integritas Dokumen Slip Gaji

Dapat dilihat bahwa dalam validasi kasus pertama, di mana tidak adanya perubahan terhadap data dokumen slip gaji, maka ketika validasi dilakukan dokumen terbukti terjaga integritasnya.

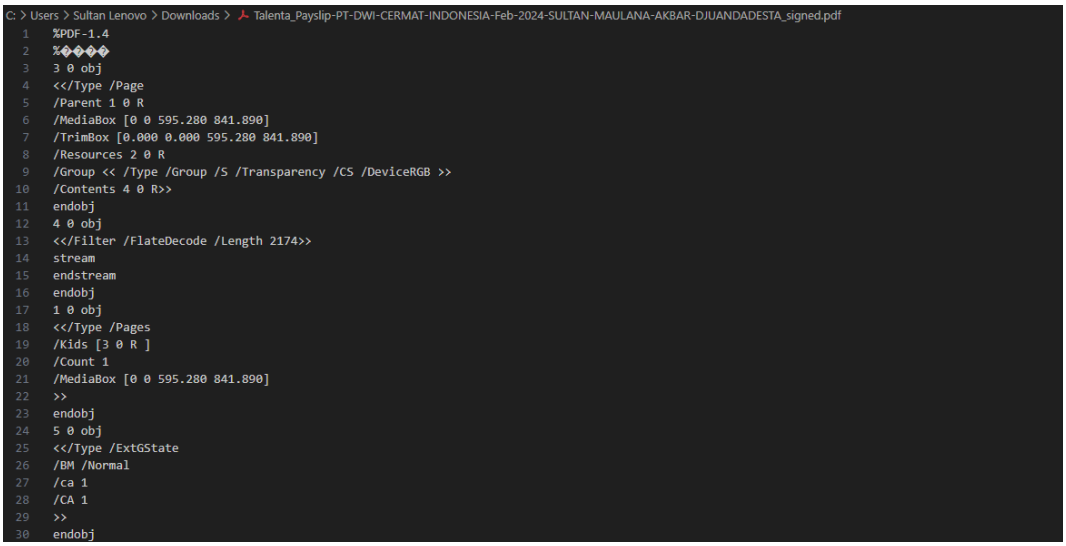
Kasus Kedua

Pada kasus kedua, dilakukan verifikasi dokumen digital yang tidak autentik dan terdapat perubahan pada tanda tangan digital yang tertanam**.** Perlu diingat terlebih dahulu bahwa perubahan tanda tangan digital yang tertanam diakibatkan oleh adanya perubahan data pada dokumen digital tersebut. Potongan layar data dokumen slip gaji tertandatangani ditampilkan pada Gambar 10 dan data dokumen tertandatangani yang telah dihapus ditampilkan pada Gambar 11. Perhatikan bahwa untuk kasus kedua ini akan tetap digunakan dokumen digital slip gaji yang telah ditandatangani pada kasus sebelumnya, tetapi akan dilakukan perubahan terhadap data dokumen digital yang sudah tertandatangani sebagai berikut.

1. Perubahan data pada dokumen slip gaji

Gambar 10. Potongan layar data dokumen slip gaji tertandatangani

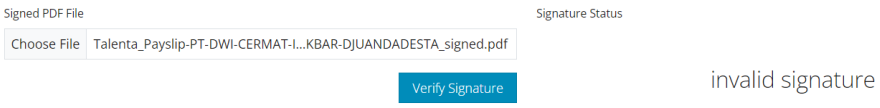
2. Perubahan data dilakukan pada data baris lima belas sampai baris 25 yang akan dihapus secara sengaja. Berikut adalah potongan layar data pada dokumen digital slip gaji yang telah dihapus sebagian secara sengaja.



Gambar 11. Data dokumen tertandatangani yang telah dihapus

3. Verifikasi dokumen slip gaji yang sengaja dirubah datanya

Setelah penghapusan secara sengaja dilakukan terhadap data yang berada pada dokumen slip gaji tertandatangani, dokumen tersebut akan disimpan dan diunggah kembali pada modul verifikasi yang tersedia pada aplikasi tanda tangan digital. Tampilan program pada Gambar 12 berikut.



Gambar 12. Hasil validasi dokumen slip gaji yang telah diubah

Dapat dilihat pada Gambar 12, ketika ada sebagian data pada dokumen digital slip gaji diubah, dalam hal ini penghapusan pada sebagian data, maka hasil validasi dari program aplikasi tanda tangan digital akan memberikan hasil invalid atau dapat disimpulkan integritas dokumen tersebut telah terganggu karena adanya perubahan tanda tangan digital yang dihasilkan oleh fungsi *hash* BLAKE2 sebelumnya.

4. KESIMPULAN

Dapat disimpulkan beberapa hal penting mengenai skema autentikasi tanda tangan digital yang menggunakan kriptografi RSA dan fungsi hash BLAKE2. Pertama, skema ini terdiri dari tiga proses utama: pembangkitan kunci, penandatanganan dokumen digital, dan verifikasi dokumen digital. Dalam proses pembangkitan kunci, dihasilkan sepasang kunci—publik untuk verifikasi dan privat untuk penandatanganan. Kedua, tanda tangan digital menggunakan fungsi hash BLAKE2 dengan skema penandatanganan RSA diterapkan pada dokumen digital berformat .pdf. Hasil penelitian menunjukkan bahwa kombinasi antara BLAKE2 dan RSA dapat memberikan keamanan untuk dokumen digital di lingkungan *cloud*.

5. DAFTAR PUSTAKA

Andreeva, E., Luykx, A., & Mennink, B. (2013). Provable Security of BLAKE with Non-ideal Compression Function. *International Conference on Selected Areas in Cryptography*, 321–338.

Aumasson, J. P., Neves, S., Wilcox-O'Hearn, Z., & Winnerlein, C. (2013). BLAKE2: simpler, smaller, fast as MD5. *International Conference on Applied Cryptography and Network Security,* 119-135. Berlin, Heidelberg: Springer Berlin Heidelberg.

Berlin, K., & Dhenakaran, S. S. (2017). An overview of cryptanalysis of RSA public key system. *International Journal of Engineering and Technology*, *9*(5), 3575-3579.

Ferreira, A., Correia, R., Antunes, L., Palhares, E., Marques, P., Costa, P., & da Costa Pereira, A. (2004). Integrity for electronic patient record reports. *Proceedings. 17th IEEE Symposium on Computer-Based Medical Systems*, 4-9. IEEE.

Firdaus, J., Marwati, R., & Muhtar, S. (2018). Penyandian pesan menggunakan kombinasi algoritma RSA yang ditingkatkan dan algoritma Elgamal. *Jurnal Eurekamatika*, 6 (1), 23–32.

Guo, J., Karpman, P., Nikolić, I., Wang, L., & Wu, S. (2014). Analysis of BLAKE2. *Cryptographers' Track at the RSA Conference*, 402-423. Cham: Springer International Publishing.

Kacha, L., & Zitouni, A. (2017). An overview on data security in cloud computing. *Proceedings of the Computational Methods in Systems and Software*, 250-261.

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace*, 2(2), 109-134.

Mouha, N., Raunak, M. S., Kuhn, D. R., & Kacker, R. (2018). Finding bugs in cryptographic hash function implementations. *IEEE Transactions on Reliability*, 67(3), 870–884.

Paul, P. K., & Ghose, M. K. (2012). Cloud Computing: possibilities, challenges and opportunities with special reference to its emerging need in the academic and working area of Information Science. *Procedia engineering*, *38*, 2222-2227.

Singh, S., Iqbal, M. S., & Jaiswal, A. (2015). Survey on techniques developed using digital signature: public key cryptography. *International Journal of Computer Applications*, *117*(16).