AUTENTIKASI DOKUMEN DIGITAL PADA *CLOUD* MENGGUNAKAN ALGORITMA *HASHING* BLAKE2 DAN RIVEST SHAMIR ADLEMAN (RSA)

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Matematika

Oleh:

Sultan Maulana Akbar Djuandadesta

1904673

PROGRAM STUDI MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2024

AUTENTIKASI DOKUMEN DIGITAL PADA CLOUD MENGGUNAKAN ALGORITMA HASHING BLAKE2 DAN RIVEST SHAMIR ADLEMAN (RSA)

Oleh
Sultan Maulana Akbar Djuandadesta

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia
September 2024

LEMBAR PENGESAHAN

SULTAN MAULANA AKBAR DJUANDADESTA

AUTENTIKASI DOKUMEN DIGITAL PADA *CLOUD* MENGGUNAKAN ALGORITMA *HASHING* BLAKE2 dan RIVEST SHAMIR ADLEMAN (RSA)

Disetujui dan disahkan,
Pembimbing I

Dra. Hj. Rini Marwati, M.S.
NIP. 196606251990012001

Pembimbing II

Hj. Dewi Rachmatin, S.Si., M.Si.
NIP. 198106282005012001

Mengetahui,
Ketua Program Studi Matematika

Dr. Katika Yulianti , S.Pd., M.Si.
NIP. 198207282005012001

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Autentikasi Dokumen Digital Pada Cloud Menggunakan Algoritma Hashing BLAKE2 dan Rivest Shamir Adleman (RSA)" beserta seluruh isinya adalah benar-benar karya saya sendiri, kecuali kutipan kutipan dari ringkasan yang semuanya telah saya jelaskan sumbernya. Apabila dikemudian hari ditemukan adanya pelanggaran, saya bersedia menanggung risiko atau sanksi yang dijatuhkan kepada saya.

Bandung, Juni 2024

Yang membuat pernyataan,

Sultan Maulana Akbar Djuandadesta

NIM. 1904673

KATA PENGANTAR

Bismillaahirrahmannirrahiim

Puji serta syukur selalu penulis panjatkan kehadirat Allah *Subhanahu wa Ta'ala* yang telah memberikan rahmat dan karunia-Nya sehinggi penulis dapat menyelesaikan skripsi yang berjudul "Autentikasi Dokumen Digital Pada Cloud Menggunakan Algoritma Hashing BLAKE2 dan RIVEST SHAMIR ADLEMAN (RSA)". Skripsi ini diajukan untuk memenuhi sebagian syarat untuk memeroleh gelar Sarjana Matematika di Universitas Pendidikan Indonesia.

Tak lupa, penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan semangat dan motivasi dalam menyelesaikan skripsi ini. Semoga Allah *Subhana wa Ta'ala* membalas kebaikan semua pihak yang telah membantu penulis dalam penyusunan skripsi ini. Harapannya, skripsi ini dapat memberikan ilmu pengetahuan mengenai penelitian yang telah dilakukan oleh penulis.

Penulis menyadari masih ada kekurangan pada pembuatan skripsi ini yang disebabkan oleh keterbatasan kemampuan penulis. Oleh karena itu, penulis sangat mengharapkan saran dan kritik yang membangun untuk menyempurnakan skripsi ini. Demikian skripsi ini penulis susun, semoga menebarkan manfaat dan mohon maaf bila masih terdapat kekurangan.

Bandung, Juni 2024

Penulis

UCAPAN TERIMA KASIH

Dengan memanjatkan puji serta syukur kehadirat Allah *Subhana wa Ta'ala* dan shalawat serta salam kepada Nabi Muhammad *Shallallahu 'Alaihi wa Sallam*, penulis dapat menyelesaikan skripsi dengan tepat waktu. Penulisan skripsi ini tidak terlepas dari dukungan, bantuan, dan doa dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tua tercinta, Ibu Reni Andeksa dan Ayah Djuanda Desta yang selalu memberikan dorongan, doa, nasihat, dan kasih sayang agar penulis selalu berusaha dengan maksimal dan senantiasa bersyukur.
2. Ibu Dra. Hj. Rini Marwati, M.S. selaku dosen Pembimbing I yang telah bersedia memberikan bimbingan, saran, kritik yang membangun, serta selalu mengawasi kemajuan proses penyusunan skripsi ini.
3. Ibu Hj. Dewi Rachmatin, S. Si, M.Si. selaku dosen Pembimbing II yang telah meluangkan waktunya untuk memberikan bimbingan dan arahan yang sangat membantu dalam penyusunan skripsi ini.
4. Bapak Dr. H. Cece Kustiawan, M.Si. selaku dosen Pembimbing Akademik yang telah mendampingi serta memberikan motivasi dan arahan yang sangat membantu sejak awal perkuliahan.
5. Seluruh dosen dan civitas academica di lingkungan Program Studi Matematika Universitas Pendidikan Indonesia
6. Seluruh rekan mahasiswa Matematika dan Pendidikan Matematika UPI 2019 yang telah menjadi temant seperjuangan terbaik dengan saling mendukung, menyemangati, dan mendoakan selama masa perkuliahan
7. Semua pihak lainnya yang tidak dapat disebutkan satu per satu yang telah memberikan dukungan secara langsun ataupun tidak langsung selama penyusunan skripsi ini.

Semoga segala bentuk dukungan, doa, dan kebaikan yang telah diberikan mendapatkan balasan berkali-kali lipat dari Allah *Subhanahu wa Ta'ala. Aamiinn.*

ABSTRAK

Di era transformasi digital, memastikan keaslian dan integritas dokumen digital menjadi sangat penting, terutama ketika dokumen digital tersebut disimpan dan diakses oleh banyak orang di *platform cloud*. Penelitian ini menyajikan solusi yang layak dan kuat untuk mengotentikasi integritas dokumen digital menggunakan fungsi hash BLAKE2 dan kriptografi RSA sebagai algoritma tanda tangan digital. BLAKE2, dikenal dengan kecepatan dan keamanannya yang tinggi, menghasilkan *hash* unik untuk setiap dokumen yang berfungsi sebagai sidik jari digital. Untuk lebih meningkatkan keamanan dan memastikan hanya pihak yang berwenang yang dapat memverifikasi keaslian dokumen, enkripsi RSA digunakan untuk melindungi hash tersebut. Penelitian ini melibatkan integrasi *hashing* BLAKE2 dan enkripsi RSA dalam lingkungan *cloud* untuk menciptakan sistem autentikasi dokumen yang aman, efisien, dan mudah diakses. Hasil penelitian menunjukkan bahwa metode yang digunakan tidak hanya memberikan jaminan keamanan yang kuat tetapi juga beroperasi secara efisien dalam lingkungan *cloud*, menjadikannya solusi yang layak bagi organisasi yang ingin melindungi dokumen digital mereka.

Kata Kunci: BLAKE2, RSA, Algoritma tanda tangan digital, Otentikasi dokumen digital

ABSTRACT

In the era of digital transformation, ensuring the authenticity and the integrity of digital document is paramount, especially when these digital documents stored and accessed by many on cloud platforms. This paper present a feasible and robust solution for authenticating the integrity of digital document utilizing BLAKE2 hash function and RSA cryptography as digital signature algorithm. BLAKE2, known for its high speed and security, generates a unique hash for each document which servers as the digital fingerprint. To further enhance security and to ensure only authorized parties can verify the document's authenticity, RSA encryption is employed to protect these hashes. Our approach involves the integration of BLAKE2 hashing and RSA encryption within cloud environment to create a secure, efficient, and accessible documen authentication system. The results show that our method not only provides strong security guarantees but also operates efficiently in a cloud context, making it a viable solution for organizations seeking to safeguard their digital documents

Keyword: *BLAKE2, RSA, Digital signature algorithm, Digital document authentication*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Adhiwijna, A. (2019). Hash Function Performance. *Hash Function Performance*, 5.

Abdulla, M., & Rana, M. (2021). Process of encryption and decryption. Retrieved July 2024, from https://www.researchgate.net/figure/Process-of-encryption-and-decryption-6_fig1_354888594.

Andreeva, E., Luykx, A., & Mennink, B. (2013). Provable Security of BLAKE with Non-ideal Compression Function. In *Springer eBooks* (pp. 321–338). https://doi.org/10.1007/978-3-642-35999-6_21

Aumasson, J., Neves, S., Wilcox-O'Hearn, Z., & Winnerlein, C. (2013). BLAKE2: Simpler, Smaller, Fast as MD5. In *Springer eBooks* (pp. 119–135). https://doi.org/10.1007/978-3-642-38980-1_8

Berlin, K., & SS, D. (2017). An Overview of Cryptanalysis of RSA Public key System. *International Journal of Engineering and Technology*, *9*(5), 3575–3579. https://doi.org/10.21817/ijet/2017/v9i5/170905312

Boneh, D. (1999). TWENTY YEARS OF ATTACKS ON THE RSA CRYPTOSYSTEM. *Notices of the American Mathematical Society*, *46*(2), 203–212. http://dbis.informatik.uni-freiburg.de/content/courses/SS09/Kursvorlesung/Theory%20I/Reading/03-RSA-survey.pdf

Burton, D. M. (2011). Elementary Number Theory Seventh Edition. New York:

Ferreira, A., Correia, R. N., Antunes, L., Palhares, E., Marques, P., Costa, P., & Da Costa Pereira, A. (2004b). *Integrity for electronic patient record reports*. https://doi.org/10.1109/cbms.2004.1311682

Firdaus, J., Marwati, R., & Muhtar, S. (2018). PENYANDIAN PESAN MENGGUNAKAN KOMBINASI ALGORITMA RSA YANG DITINGKATKAN DAN ALGORITMA ELGAMAL. *PENYANDIAN PESAN MENGGUNAKAN KOMBINASI ALGORITMA RSA YANG DITINGKATKAN DAN ALGORITMA ELGAMAL*, *6*(1), 23–32. http://ejournal.upi.edu/index.php/JEM/article/view/11653

Hłobaż, A. (2023). Analysis of the possibility of using selected hash functions submitted for the SHA-3 competition in the SDEX encryption method.

International Journal of Electronics and Telecommunications. https://doi.org/10.24425/ijet.2022.139848

Kacha, L., & Zitouni, A. (2017). An Overview on Data Security in Cloud Computing. In *Advances in intelligent systems and computing* (pp. 250–261). Springer Nature. https://doi.org/10.1007/978-3-319-67618-0_23

Kapoor, B., & Pandya, P. (2014). Data Encryption. In *Elsevier eBooks*. https://doi.org/10.1016/b978-0-12-416681-3.00002-1

Lakha, S., & Taneja, P. (2009b). Balancing Democracy and Globalisation: The Role of the State in Poverty Alleviation in India. *South Asia-journal of South Asian Studies*. https://doi.org/10.1080/00856400903374319

Lian, S., Sun, J., & Wang, Z. (2006). Secure hash function based on neural network. Neurocomputing, 69(16–18), 2346–2350. https://doi.org/10.1016/j.neucom.2006.04.003

Makhtoum, H. E., & Bentaleb, Y. (2021). An improved IOT Authentication Process based on Distributed OTP and Blake2. International Journal of Wireless and Microwave Technologies, 11(5), 1–8. https://doi.org/10.5815/ijwmt.2021.05.01

Marković, D., Zivkovic, D., Branovic, I., Popovic, R., & Cvetković, D. (2013). Smart power grid and cloud computing. *Renewable & Sustainable Energy Reviews*, *24*, 566–577. https://doi.org/10.1016/j.rser.2013.03.068

Mallik, A. (2019). MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. Cyberspace: Jurnal Pendidikan Teknologi Informasi. https://doi.org/10.22373/cj.v2i2.3453.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. https://doi.org/10.6028/nist.sp.800-145

Munir, R. (2004). Teori Bilangan (Number Theory) Bahan Kuliah IF5054.

Munir, R. (2006). Kriptografi. Bandung: Informatika Bandung.

Nia, M. A., Sajedi, A., & Jamshidpey, A. (2014). An introduction to digital signature schemes. *arXiv (Cornell University)*. https://arxiv.org/pdf/1404.2820.pdf

Paar, C., & Pelzl, J. (2009). *Understanding Cryptography: A Textbook For Students And Practitioners*. http://euro.ecom.cmu.edu/resources/elibrary/epay/Sigs.pdf

Paul, P., & 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. https://doi.org/10.1016/j.proeng.2012.06.267

Singh, S. V., Iqbal, M. S., & Jaiswal, A. (2015). Survey on Techniques Developed using Digital Signature: Public key Cryptography. *International Journal of Computer Applications*, *117*(16), 1–4. https://doi.org/10.5120/20635-3272

Singh, S., Iqbal, M., & Jaiswal, A. (2015). Survey on Techniques Developed using Digital Signature: Public key Cryptography. International Journal of Computer Applications, 117, 1-4. https://doi.org/10.5120/20635-3272.

Stinson, D. R., & Paterson, M. B. (2018). *Cryptography: Theory and Practice*. Textbooks in Mathematics.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds. *Computer Communication Review*, *39*(1), 50–55. https://doi.org/10.1145/1496091.1496100