BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Pada abad ke-21 ini manusia telah berkembang pesat khususnya pada bidang teknologi dan informasi. Globalisasi bidang teknologi dan informasi telah menciptakan sebuah gagasan *borderless world* atau dunia tanpa batas di mana batasan-batasan geografis dan nasional semakin tidak relevan. Konsep tersebut mencerminkan pandangan terhadap hambatan-hambatan terhadap aliran modal, teknologi, serta informasi akan diminimalkan atau bahkan dihilangkan sepenuhnya (Lakha & Taneja, 2009).

Sebagai hasilnya, inovasi dan perkembangan bisnis pada abad ke-21 ini menjadi semakin pesat dan terwujudnya kolaborasi global yang lebih luas dan menciptakan berbagai macam dampak positif bagi umat manusia dalam bidang teknologi dan informasi. Salah satu jejak atau bukti evolusi manusia pada bidang teknologi dan informasi adalah komputasi awan atau *cloud computing***.** Komputasi awan atau *cloud computing* adalah penggunaan sumber daya komputasi (*hardware* dan *software*) yang dijadikan sebagai sebuah layanan melalui jaringan, seperti internet (Kacha & Zitouni, 2017), komputasi awan atau *cloud computing* juga didefinisikan sebagai mekanisme atau model yang memungkinkan akses jaringan yang mudah, nyaman, dan sesuai permintaan terhadap sebuah kumpulan perangkat seperti server, jaringan/*network*, perangkat penyimpanan, aplikasi, dan perangkat komputasi canggih lainnya (Paul & Ghose, 2012).

Terintegrasinya penggunaan komputasi awan atau *cloud computing* dalam kehidupan sehari-hari menuntut manusia untuk bertukar informasi secara digital. Salah satu bentuk pertukaran informasi yang dilakukan secara digital adalah penggunaan dokumen digital. Dokumen digital adalah sebuah dokumen dalam format atau bentuk elektronik, seperti pdf, txt, dan docx yang dibuat, disimpan, dan didistribusikan melalui perangkat elektronik atau perangkat teknologi informasi. Dokumen digital digunakan sebagai sarana penyimpanan informasi sensitif dan non sensitif yang kemudian diunggah atau disebarluaskan melalui awan atau *cloud*. Akan tetapi, sebuah dokumen digital memiliki sifat terbuka atau dapat dibaca dan diubah oleh pihak yang tidak berhak sehingga rentan terhadap perubahan dokumen secara tidak sah pada proses transfer atau penyimpanan.

Salah satu bentuk kasus yang terjadi dalam dunia nyata adalah indikasi *fraud* atau kecurangan yang dilakukan oleh pelanggan *Online Travel Agent* (OTA) dalam melakukan klaim *refund* sebuah pemesanan. *Fraud* atau kecurangan tersebut dilakukan dengan merubah informasi pada dokumen digital .pdf tiket pelanggan dengan informasi lain yang mendukung argumen palsu dari pelanggan terkait. Hal ini dapat menyebab kerugian finansial yang harus diterima perusahaan sebagai konsekuensi ketidakadaannya sistem validasi terhadap keintegritasan sebuah dokumen digital.

Oleh karena itu, untuk melindungi dokumen digital yang diunggah atau disebarluaskan pada awan atau *cloud* dari berbagai jenis perilaku *fraud* atau serangan siber yang dapat mengubah keaslian dokumen, seperti serangan *Man in the Middle* (MitM) yang melibatkan pihak luar yang tidak disetujui memasuki jaringan dan mengubah informasi sensitif tanpa sepengetahuan pengguna (Mallik, 2019). Oleh karena itu, diperlukan sebuah upaya perlindungan integritas dokumen dengan ilmu kriptografi. Ilmu kriptografi adalah elemen penting dalam melindungi dokumen digital dari ancaman yang dapat merusak keaslian dan integritasnya.

Dokumen-dokumen digital memiliki sifat yang terbuka dan rentan terhadap perubahan oleh pihak yang tidak berhak, terutama selama proses transfer atau penyimpanan dalam lingkungan awan atau cloud. Ancaman seperti serangan MitM dapat mengubah dokumen secara tidak sah, dan itulah mengapa perlindungan integritas dokumen melalui tanda tangan digital menjadi krusial. Tanda tangan digital adalah sebuah metode yang memastikan bahwa dokumen digital tetap otentik dan tidak mengalami perubahan yang tidak sah. Ilmu kriptografi berperan besar dalam implementasi tanda tangan digital, termasuk penggunaan enkripsi dengan kriptografi kunci simetri, enkripsi dengan kunci publik, dan tanda tangan menggunakan kriptografi kunci publik serta fungsi hash.

Teknik tanda tangan digital berbasis kriptografi kunci publik, seperti yang dikemukakan oleh Singh et al. (2015), memberikan platform yang aman untuk pertukaran data, verifikasi integritas, dan pembuktian identitas pengirim, menjadikan kriptografi sebagai pilar penting dalam era digital ini. Tanda tangan digital adalah sebuah metode untuk memastikan keaslian dan integritas dari sebuah dokumen digital. Ferreira et al. (2004) mengatakan bahwa tanda tangan digital

dapat memberikan kepercayaan yang nyata dengan mencegah dan mendeteksi ketidaksesuaian atau kesalahan yang dapat mempengaruhi integritas informasi.

Metode tanda tangan digital umumnya melibatkan penggunaan ilmu kriptografi, di antaranya dengan melakukan enkripsi dengan kriptografi kunci simetri, enkripsi dengan kunci publik, atau tanda tangan dengan menggunakan kriptografi kunci publik dan fungsi *hash* (Munir, 2004). Menurut Singh et al. (2015), teknik tanda tangan digital berbasis kriptografi kunci publik menyediakan platform yang lebih baik dalam pertukaran dan penyimpanan data yang aman, verifikasi integritas, dan membuktikan identitas pengirim.

Fungsi *hash* adalah suatu fungsi yang menerima masukan berupa string yang panjangnya sembarang dan mengonversi masukan tersebut menjadi string yang mempunyai panjang tetap (*fixed*) dan umumnya menjadi lebih kecil dari panjang semula (Munir, 2004). Stinson dan Paterson (2018) juga menjelaskan, fungsi *hash* digunakan untuk membuat "*fingerprint*" singkat dari beberapa data; jika data tersebut diubah, maka sidik jari tersebut tidak akan lagi valid. Misalkan sidik jari tersebut disimpan di tempat yang aman. Maka, meskipun data disimpan di tempat yang tidak aman, integritasnya dapat diperiksa dari waktu ke waktu dengan menghitung ulang sidik jari dan memverifikasi bahwa sidik jari tersebut tidak berubah.

Fungsi *hash* merupakan fungsi satu arah yang memiliki keamanan terhadap MitM sehingga cocok untuk digunakan dalam proses otentikasi (Lian et al., 2006). *Output* atau keluaran yang dihasilkan dari penggunaan fungsi *hash* disebut dengan nilai *hash* atau pesan ringkas (*message digest*). Nilai *hash* memiliki karakteristik unik dan jika terdapat sedikit saja perubahan pada *input* maka nilai *hash* yang dihasilkan akan jauh berbeda. Dengan menggunakan fungsi *hash*, informasi dari sebuah dokumen digital dapat direpresentasikan dengan singkat & efisien sehingga cocok untuk dapat digunakan sebagai *identifier* atau tanda pengenal unik dari sebuah dokumen.

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., 2013b).

Dibandingkan dengan fungsi *hash* lainnya, BLAKE2 lebih cepat daripada MD5, memberikan keamanan yang serupa dengan SHA-3: dengan *collision resistance* 256-bit dan memiliki kekebalan terhadap *length extension* (Aumasson et al., 2013b). Didukung juga oleh analisis dan riset yang telah dilakukan, BLAKE2 memiliki margin keamanan yang sangat tinggi terhadap semua serangan yang diketahui (Guo et al., 2014), memiliki ketahanan terhadap serangan *brute force* (Adhiwijna, 2019), dan secara optimal aman terhadap *collision*, *second preimage*, dan *preimage* (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). Kriptosistem RSA biasa digunakan untuk memberikan privasi dan memastikan keaslian dari sebuah data digital (Boneh, 1999) dan menurut makalah *An Overview of Cryptanalysis of RSA Public key System* yang ditulis oleh Berlin dan SS (2017) sistem kriptografi RSA masih merupakan keamanan yang baik untuk mengirimkan *sensitive data*.

Proses *digital signature* atau penandatangan memerlukan sebuah fungsi *hash* yang memenuhi tiga kriteria, yaitu memiliki ketahanan *preimage* (resistensi *preimage*), ketahanan *preimage* kedua, dan ketahanan *collision* yang kuat (Kapoor & Pandya, 2014) dan tanda tangan digital berbasis kriptografi kunci publik menyediakan platform yang lebih baik untuk pertukaran dan penyimpanan data yang aman, memastikan integritas dan membuktikan identitas pengirim (Singh et

al., 2015). Oleh karena itu, penulis tertarik untuk melakukan penelitian tentang autentikasi dokumen digital pada *cloud* menggunakan algoritma *hashing* BLAKE2 dan RSA.

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. Pada penelitian sebelumnya, belum pernah ada yang meneliti tentang implementasi BLAKE2 yang dikombinasikan dengan kriptograsi RSA pada *cloud* yang menciptakan dimensi baru dalam pemrosesan dan penyimpanan dokumen digital dengan menitikberatkan pada kecepatan, efisiensi, dan keamanan. Penelitian ini melibatkan aplikasi konkret dari 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 dengan penelitian ini, peneliti berharap dapat memberikan manfaat teoritis dan praktis terhadap pengamanan integritas sebuah dokumen digital dan keberlanjutan penggunaannya dalam konteks teknologi informasi modern.

1.2 Rumusan Masalah Penelitian

Dari pemaparan latar belakang di atas, diperoleh rumusan masalah sebagai berikut:

1. Bagaimana skema autentikasi menggunakan algoritma *hashing* BLAKE2 dan skema kriptografi RSA?
2. Bagaimana konstruksi program aplikasi *digital signature* menggunakan kriptografi RSA dan fungsi *hash* BLAKE2 pada *cloud*?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah, dokumen penandatangan digital terbatas hanya untuk *file* dengan ekstensi .pdf

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya, maka tujuan dari penelitian ini adalah:

1. Implementasi skema penandatanganan digital dengan fungsi *hash* BLAKE2 dan algoritma kriptografi RSA untuk dokumen digital berekstensi .pdf
2. Membuat program aplikasi *digital signature* menggunakan fungsi *hash* BLAKE2 dan algoritma kriptografi RSA pada *environment* awan atau *cloud*?

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah:

1. Manfaat Teoritis

   Secara teoritis hasil dari penelitian ini akan bermanfaat bagi bidang kriptografi khususnya tentang *digital signature*. Adapun manfaat tersebut ialah:

   a. Memberikan pemahaman skema penandatangan dengan algoritma RSA
   b. Memberikan pemahaman fungsi *hash* BLAKE2 untuk *digital signature*

2. Manfaat Praktis

   Dalam praktiknya hasil penelitian ini diharapkan memberikan program penandatanganan dengan fungsi *hash* BLAKE2 dan kriptografi RSA juga implementasinya pada awan atau *cloud*.