BAB I
PENDAHULUAN

1.1 Latar Belakang

Cloud computing adalah model komputasi yang dikembangkan dimana sumber daya dari infrastruktur komputasi di sediakan melalui internet (Bhangotra & Puri, 2015). Penggunaan *cloud computing* memberikan kemudahan dan keuntungan diantaranya dapat mengurangi biaya komputasi, format dokumen yang lebih baik, kapasitas penyimpanan tidak terbatas dan lainnya (Mohamed, Abdelkader, & El-Etriby, 2012). Walaupun demikian *cloud computing* bukan tanpa kelemahan. Menurut Kadlag & Paikrao (2014) mengungkapkan beberapa kelemahan dari *cloud computing* diantaranya : keamanan data, sistem *backup file*, keamanan lalu lintas jaringan dan teknik enkripsi kriptografi tentu saja merupakan praktik terbaik untuk mengatasi masalah keamanan.

Salah satu penyedia layanan *cloud computing* adalah Dropbox. Dropbox menyediakan layanan penyimpan *online* gratis maupun berbayar. Dropbox menawarkan jumlah pengguna yang relatif besar, dengan penggunaan sistem operasi yang bervariasi, baik untuk perangkat *mobile* ataupun desktop, hadir hampir disemua sistem operasi populer, *Dropbox for windows*, *Dropbox for iOS Dropbox for android*, *Dropbox for mac*, *Dropbox for Ubuntu*.

Namun demikian Dropbox bukanlah layanan tanpa kelemahan. Mulazzani, Schrittwieser, Leithner, Huber, & Weippl (2011) menganalisis perangkat lunak klien Dropbox serta protokol transmisinya, menunjukkan kelemahan dan menjelaskan kemungkinan vektor serangan terhadap klien. Mereka melakukan tiga serangan terhadap Dropbox. Serangan pertama yaitu *Hash Value Manipulation Attack* dilakukan dengan memodifikasi kode sumber *NCrypto* yang tersedia untuk publik sehingga menggantikan nilai *hash* yang dihitung oleh OpenSSL dengan nilai mereka sendiri, membuatnya dan menggantikan pustaka yang dikirimkan dengan Dropbox. Karena manipulasi nilai *hash* mereka dapat mengakses *file* klien, serangan ini tidak terdeteksi oleh klien maupun pihak Dropbox. Serangan kedua yaitu *Stolen Host ID Attack*, dengan serangan ini semua *file* di akun

klien dapat diunduh oleh penyerang. Serangan ini hanya terdeteksi oleh server Dropbox dan tidak terdeteksi oleh klien. Serangan ketiga *Direct Download Attack*, dengan serangan ini penyerang dapat akses ke *file*

klien dan terdeteksi oleh server Dropbox tetapi tidak terdeteksi oleh klien.

Beberapa tahun terakhir Dropbox beberapa kali dikabarkan telah diretas. Pada bulan oktober 2014 seseorang mengaku telah meretas akun Dropbox melalui akun Raddit, ia mengaku memiliki 7 juta *username*. Peretas tersebut membagikan ratusan *username* dalam sebuah *text file*, namun pihak Dropbox menyangkal bahwa keamanan mereka berhasil diretas, *username* tersebut dicuri dari layanan lain dan digunakan untuk *login* ke akun Dropbox (Reilly, 2014). Kabar peretasan terhadap Dropbox juga terjadi pada tahun 2012 Sekitar 68 juta akun klien, Dropbox mengungkapkan bahwa peretas telah mengakses sistem internalnya dan mengakses daftar akun *email* klien, namun tidak mengatakan termasuk kata sandi. Agustus 2016 Motherboard, pakar keamanan Troy Hunt dan Leaked Source layanan pemberitahuan keamanan, masing-masing melaporkan bahwa peretasan pada tahun 2012 tersebut termasuk email dan kata sandi (Hautala,2016).

Secara umum, penyerangan terhadap media penyimpanan *online* dapat dibagi kedalam dua cara yaitu serangan dari luar dan serangan dari dalam. Serangan dari luar dapat dilakukan oleh *hacker* dengan cara meretas sistem internal penyimpanan *online* sedangkan serangan dari dalam dapat dilakukan oleh administrator penyedia layanan, administrator bisa memiliki kemungkinan untuk *hack* data pengguna, serangan dari dalam sangat sulit untuk di identifikasi sehingga harus berhati-hati saat menyimpan data di penyimpanan *online*. Hal ini juga diungkapkan oleh Kaur & Bhardwaj (2012) meski datanya dapat diakses oleh pihak ketiga, mereka seharusnya tidak mendapatkan data sebenarnya jadi semua data harus dienkripsi sebelum dikirim ke penyimpanan *online*.

Teknik enkripsi tersebut dipelajari dalam ilmu kriptografi. Kriptografi adalah seni dan sains untuk mencapai keamanan dengan menyandikan pesan agar tidak terbaca (Sharma & Gupta, 2017). Algoritma yang digunakan untuk proses enkripsi dan dekripsi terdiri dari algoritma dengan kunci simetri dan asimetri. Algritma kunci simetri dan asimetri mempunyai kelebihan dan kekurangannya masing-masing. Kunci simetri dalam pengaplikasiannya lebih cepat daripada asimetri tetapi semua pihak harus membagikan kuncinya kepada *public* sehingga rentan keamanannya sedangkan kunci asimetri mempunyai tingkat kamanan yang lebih tatapi dalam pengimplemtasiannya membutuhkan waktu yang lama (Indu, Anand, & Shaji, 2017) .

Berdasarkan uraian permasalahan tersebut, maka dilakukan penelitian cara menghindari bahaya pencurian atau kebocoran data pada

penyimpanan *cloud computing* dengan cara mengenkripsi *file* sebelum dikirim ke penyimpanan cloud. Pada penelitian ini layanan *cloud* yang digunakan adalah Dropbox, *file* yang akan di disimpan ke penyimpanan Dropbox akan di enkripsi terlebih dahulu, sehingga jika terjadi peretasan terhadap sistem Dropbox, *file* yang tersimpan akan tetap aman meskipun data berhasil diakses oleh peretas dari server Dropbox, peretas tidak dapat mengerti maknanya karena data yang tersimpan terenkripsi dan hanya pemilik *file* saja yang mempunyai kunci untuk mendekripsi *file*, bahkan pihak Dropbox tidak dapat mendekripsi *file* tersebut. Cara ini juga dapat menghindarkan serangan dari dalam yaitu penyalagunaan data oleh pihak penyedia layanan *cloud* mengingat penyedia layanan *cloud* dapat mengakses data klien.

Penelitian ini menerapkan teknik kriptografi *hybrid cryptosystem*. *Hybrid cryptosystem* adalah teknik menggabungkan algoritma simetri dan asimetri, menggunakan keamanan dan kecepatan simetri bersama kekuatan asimetri dalam mendistribusikan kunci yang aman (Torkaman, Nikfard, Kazazi, Abbasy, & Tabatabaiee, 2011). Algoritma simetry yang digunakan adalah algoritma *Twofish*. Pada penelitian sebelumnya yang dilakukan oleh Rizvi, Hussain, & Wadhwa (2011) menyimpulkan bahwa algoritma *Twofish* merupakan algoritma yang cepat dalam proses enkripsi dan dekripsi, sederhana dan memiliki keamanan yang tinggi untuk diterapkan. Mereka menganalisis AES dan *Twofish*, hasil menunjukkan bahwa faktor keamanan *Twofish* lebih besar dari AES. Dari hasil simulasi dapat juga disimpulkan bahwa *Twofish* lebih cepat dari AES. Hasil penelitian ditujukan pada Tabel 1.1 dan Tabel 1.2.

Tabel 1.1 Perbandingan Konsumsi Waktu Algoritma *Twofish* dan AES

Plain text Size in Mbytes	**1GB RAM**		**2GB RAM**		**3GB RAM**	
	Twofish	**AES**	***Twofish***	**AES**	***Twofish***	**AES**
1.31	109	120	89	118	76	117
1.52	172	183	152	182	134	179
2.03	204	222	194	219	174	218
2.79	232	245	202	243	187	241
3.01	282	301	252	299	242	298
7.13	532	539	492	537	465	535
13.50	756	764	686	761	665	759

Plain text Size in Mbytes	**1GB RAM**		**2GB RAM**		**3GB RAM**	
	Twofish	**AES**	***Twofish***	**AES**	***Twofish***	**AES**
Average time (sec)	2487	2374	2067	2359	196553	2347
Execution speed	12.58	13.1803	15.18	13.264	16.046	13.13

Sumber : Rizvi, Hussain, & Wadhwa, 2011

Tabel 1. 2 Pebandingan Keamanan *Twofish* dan AES

AES	1.11/1.33/1.56
Twofish	2.67
18-round AES	2.00
24-round AES	2.67

Sumber : Rizvi, Hussain, & Wadhwa, 2011

Sedangkan algoritma asimetri yang akan digunakan untuk mengenkripsi kunci *Twofish* adalah RSA. RSA adalah singkatan dari tiga penemunya yaitu Ron Rivest, Adi Shamir dan Leonard Adleman(Sharma & Gupta, 2017). RSA merupakan salah satu kunci publik yang paling dikenal cryptosystem untuk pertukaran kunci, tanda tangan digital atau enkripsi blok data (Singh, 2013). Pada penelitian sebelumnya yang dilakukan oleh Indu et al., (2017) menganalisis kinerja dari RSA, Elgamal dan Pallier. Dari hasil penelitian disimpulkan bahwa RSA berkinerja baik dalam penanganan ukuran *file* kecil. Hasil penelitian sebelumnya ditunjukan pada Tabel 1.3

Tabel 1. 3 Pebandingan Algoritma Asimetri

Algoritma	Waktu Enkripsi(ms)	Waktu Dekripsi (ms)	Ram yang digunakan (%)	Memori yang digunakan (%)
Elgamal	35	13	44	18
Paillier	47	12	40	16
RSA	9	8	16	10

Sumber: Indu et al., 2017

Pada penelitian ini, algoritma *Twofish* akan digunakan sebagai pengamanan *file* yang akan disimpan di *cloud*. Sedangkan algoritma RSA akan digunakan untuk pengamanan kunci dari algoritma *Twofish*. Penerapan *hybrid cryptosystem Twofish* dan RSA ini diharapkan dapat mengamankan data yang akan disimpan di penyimpanan cloud.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka dapat dirumuskan permasalahan sebagai berikut.

1. Bagaimana mengimplementasikan *hybrid crytosystem* algoritma *Twofish* dan RSA dalam penyandian *file* untuk mengamankan *file* yang akan disimpan dan dikirim kepengguna lain di *cloud computing*?
2. Bagaimana hasil penerapan *hybrid crytosystem* algoritma *Twofish* dan RSA terhadap kerahasiaan data berdasarkan pengujian *avalanche effect* dan *randomness* terhadap *ciphertext* hasil enkripsi?
3. Bagaimana hasil pengujian terhadap perubahan ukuran *file* dan lama waktu proses dalam penerapan *hybrid cryptosystem* algoritma *Twofish* dan RSA pada berbagai ukuran *file*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan penelitian adalah sebagai berikut.

1. Mengimplementasikan *hybrid cryptosystem* algoritma *Twofish* dan RSA pada penyandian *file* untuk mengamankan *file* yang akan simpan dan dikirim ke pengguna lain di *cloud computing*.
2. Mengetahui hasil penerapan *hybrid cryptosystem* algoritma *Twofish* dan RSA terhadap kerahasiaan data berdasarkan

pengujian *avalanche effect* dan *randomness* terhadap *ciphertext* hasil enkripsi.

3. Mendapatkan data perubahan ukuran *file* dan lama waktu proses dalam penerapan *hybrid cryptosystem* algoritma *Twofish* dan RSA pada berbagai ukuran *file.*

1.4 Batasan Masalah

Pada penelitian ini, permasalahan dibatasi hal-hal berikut ini.

1. *Cloud computing* yang digunakan adalah Dropbox.
2. Data yang di digunakan untuk di enkripsi hanya *file* *.doc.
3. Pengujian *randomness test* terhadap kerahasiaan data algoritma *Twofish* dan RSA dilakukan dengan bantuan *software* Cryptool 1.4.3.
4. Proses enkripsi dilakukan sebelum data di*upload* ke penyimpanan *cloud*.
5. Proses deskripsi dilakukan setelah data di*download* dari penyimpanan *cloud*.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diambil dari hasil penelitian ini adalah sebagai berikut.

1. Bagi Peneliti
   Dapat menambah ilmu pengetahuan peneliti tentang *hybrid cryptosystem* dan penerapannya untuk kasus di kehidupan nyata khususnya dalam kasus keamanan penyimpanan data pada *cloud computing*
2. Bagi Universitas
   a. Dapat menjadi sumbangan karya ilmiah disiplin ilmu kriptografi, penyimpanan *cloud computing*.
   b. Dapat dijadikan sebagai bahan acuan bagi peneliti lain yang akan mengkaji permasalah dengan topik yang serupa.
3. Bagi pengguna cloud Dropbox
   Dapat digunakan untuk meningkatkan keamanan *file* yang akan disimpan di penyimpanan Dropbox
4. Bagi pengembang teknologi
   Dapat mengetahui kelebihan dan kekurangan metode *hybrid cryptosystem Twofish* dan RSA dalam pengamanan *file*.

1.6 Sistematika Penulisan

Berikut ini adalah sistematika penulisan yang dilakukan dalam menyusun skripsi :

BAB I PENDAHULUAN

Bab ini berisikan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan masalah, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas mengenai teori-teori dasar yang terkait dalam penelitian, yaitu teori tentang *cloud computing,*kriptograpi,hybrid cryptosystem.

BAB III METODELOGI PENELITIAN

Bab ini menguraikan metode yang digunakan dalam penelitian secara rinci, baik dalam pengumpulan data maupun tahap pembuatan perangkat lunaknya.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi uraian tentang hasil penelitian dan pembahasan terhadap hasil penelitian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari keseluruhan penelitian yang telah dilakukan, serta saran dari penulis untuk kegiatan penelitian selanjutnya terkait dengan topik yang sedang dibahas.