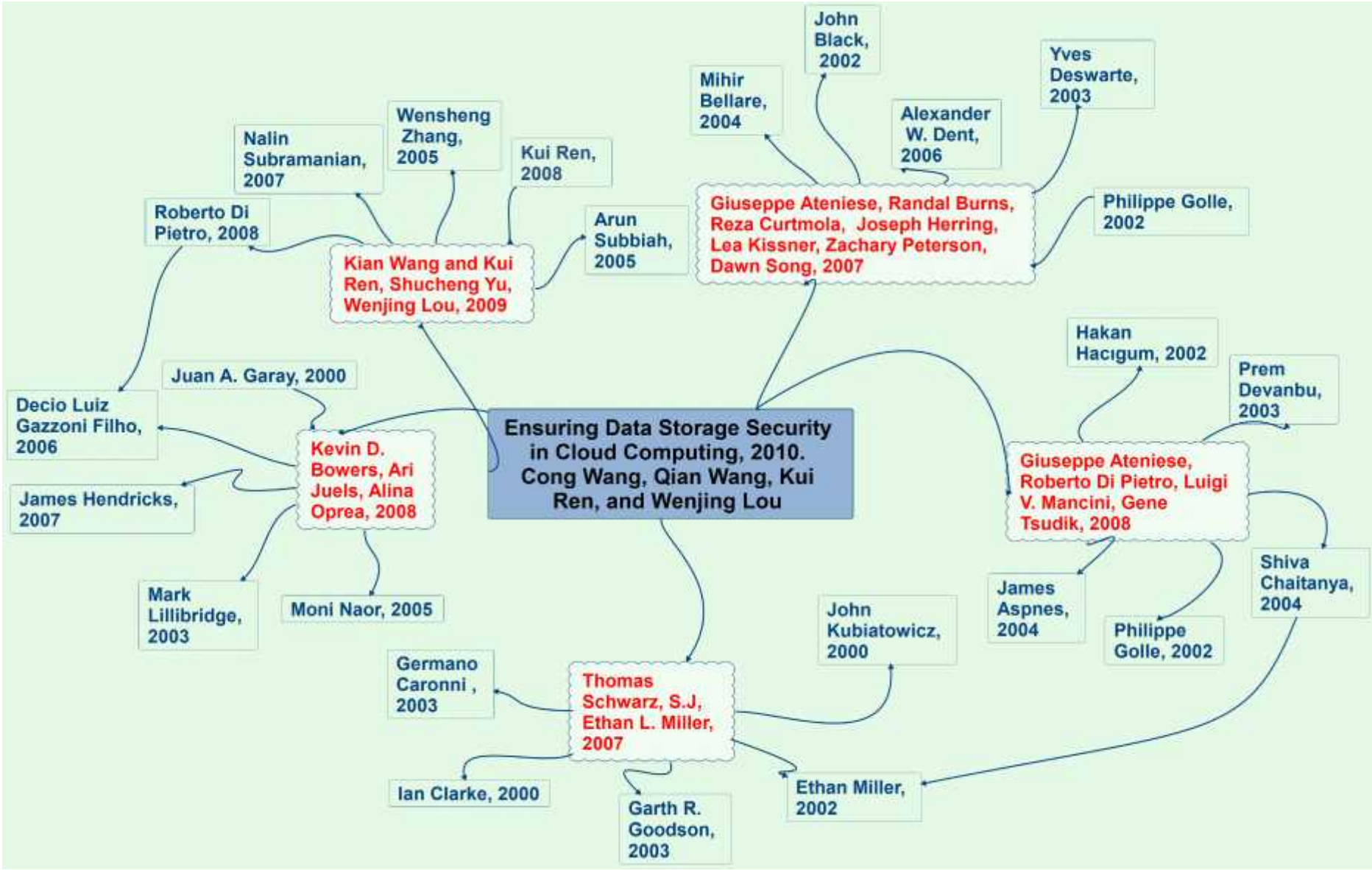
TEKNIK PENULISAN KARYA ILMIAH

OLEH

FERLITA PRATIWI ARISANTI
09011181520015
SK2A

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2016


Ensuring Data Storage Security in Cloud Computing, 2010. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou
Kian Wang and Kui Ren, Shucheng Yu, Wenjing Lou, 2009
Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, Dawn Song, 2007
Kevin D. Bowers, Ari Juels, Alina Oprea, 2008
Giuseppe Ateniese, Roberto Di Pietro, Luigi V. Mancini, Gene Tsudik, 2008
Thomas Schwarz, S.J, Ethan L. Miller, 2007
John Black, 2002
Mihir Bellare, 2004
Yves Deswarte, 2003
Alexander W. Dent, 2006
Philippe Golle, 2002
Wensheng Zhang, 2005
Nalin Subramanian, 2007
Kui Ren, 2008
Roberto Di Pietro, 2008
Arun Subbiah, 2005
Hakan Hacıgum, 2002
Prem Devanbu, 2003
Shiva Chaitanya, 2004
James Aspnes, 2004
Philippe Golle, 2002
John Kubiatowicz, 2000
Ethan Miller, 2002
Juan A. Garay, 2000
Decio Luiz Gazzoni Filho, 2006
James Hendricks, 2007
Mark Lillibridge, 2003
Moni Naor, 2005
Germano Caronni , 2003
Ian Clarke, 2000
Garth R. Goodson, 2003

KESIMPULAN

Pada paper Ensuring Data Storage Security in Cloud Computing tahun 2010 oleh Cong Wang, Qian Wang, Kui Ren, and Wenjing Louy, dapat ditarik kesimpulan cloud computing atau yang biasa disebut dengan komputasi awan di dalam paper ini penulis menyelidiki masalah keamanan penyimpanan data di dalam cloud computing yang pada dasarnya disalurkan didalam penyimpanan. Untuk memastikan kebenaran pada pengguna di dalam penyimpanan data cloud computing, paper ini mengemukakan skema yang dibagi secara efektif dan fleksibel dengan pendukung data dinamik yang jelas, termasuk update, menghapus, dan menambahkan. Dan juga mengandalkan kode penghapusan dalam penyusunan distribusi file untuk memberikan redundansi vektor paritas dan menjamin keandalan data.

Cloud computing merupakan sebuah area yang penuh dengan tantangan yang sangat penting, hingga saat ini masih dalam penelitian dan banyak masalah dalam penelitian yang belum diidentifikasi. Ketika sudah memutuskan untuk adopsi atau migrasi data ke Cloud, yang harus diperhatikan adalah bagaimana penyedia layanan Cloud memberikan proteksi terhadap data. Dengan metode apa mereka melakukan proteksi sehingga yakin data aman, selain itu lokasi penyimpanan data juga adalah pertimbangan penting dimana ini hubungannya dengan Data Center. Dipastikan data center yang mereka buat sudah tersertifikasi atau teraudit. Setelah data terproteksi, selanjutnya adalah bagaimana keamanan dari akses terhadap data (role), bagaimana prosedurnya sehingga hanya orang-orang yang berhak saja yang bisa akses data kita. Salah satu sifat Cloud computing adalah resource sharing. Infrastruktur cloud computing yang memungkinkan akses dan penggunaan secara bersamanmenimbulkan masalah privasi data. Ancaman privasi data dapat berasal dari pihak internal (penyedia layanan, pengguna dalam perusahaan), dan kebocoran data bisa terjadi karena kegagalan hak akses keamanan di beberapa domain. Dari sudut pandang pengguna layanan cloud itu sendiri harus mempertimbangkan beberapa hal penting seperti : kontrol terhadap sistem dan data, menciptakan fasilitas untuk penggunaan banyak identitas dan membatasi informasi identitas serta autentifikasi untuk transaksi tingkat tinggi atau yang dianggap penting. Semua hal tersebut yang harus dijamin bagi seorang individu agar privasi informasi yang disampaikan kepada cloud provider dapat dipastikan aman.

Pada paper tersebut mensitasi dari Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance pada tahun 2009 oleh Qian Wang dan Kui Ren, Baru-baru ini, penyimpanan data telah mendapatkan peningkatan dalam popularitas untuk manajemen data

yang efisien dan kuat dalam jaringan sensor nirkabel (WSNs). arsitektur terdistribusi untuk membangun sistem penyimpanan data yang sangat aman dan dapat diandalkan namun tetap aman. Pada paper ini, skema penyimpanan data yang aman dan dapat diandalkan dengan jaminan integritas dinamis dalam jaringan sensor nirkabel. Dengan memanfaatkan berbagi penghapusan coding dalam proses penyimpanan data awal untuk menjamin kerahasiaan data dan kehandalan pada data. Berdasarkan prinsip bagi rahasia dan penghapusan coding.

Kemudian mensitasi dari Paper HAIL: A High-Availability and Integrity Layer for Cloud Storage tahun 2008 oleh Kevin D. Bowers, Ari Juels dan Alina Oprea, paper ini mengenalkan ketersediaan dan integritas pada Layer. Pada sistem kriptografi terdistribusi yang memungkinkan satu server untuk membuktikan kepada klien bahwa file yang tersimpan utuh dan dapat diambil. HAIL meningkatkan pada keamanan dan efisiensi alat yang ada, seperti Bukti Retrievability (Pors) ditempatkan pada setiap server. Kemudian diimplementasikan ke dalam prototipe. HAIL merupakan remote file yang mengintegritas protokol pemeriksaan yang menawarkan efisiensi, keamanan, dan perbaikan modeling.

Pada paper Using Algebraic Signatures to Check Remotely Administered Storage tahun 2007 oleh Schwarz, Thomas S. J, Miller, Ethan L, Munculnya penggunaan Internet untuk penyimpanan jarak jauh dan dan cadangan telah menyebabkan masalah memverifikasi bahwa situs penyimpanan dalam sistem terdistribusi memang telah menyimpan data. Ini harus sering dilakukan. Pada paper tersebut menggunakan metode penghapusan dan mengoreksi coding untuk menjaga data yang disimpan dengan menggunakan tanda tangan aljabar. fungsi hash pada aljabar properti untuk verifikasi.

Scalable and Efficient Provable Data Possession tahun 2008 oleh Giuseppe Ateniese, Roberto Di Pietro, Luigi V. Mancini, Penyimpanan outsourcing yang mendorong sejumlah masalah keamanan yang menarik. Namun, dapat dibuktikan data Possession (PDP) adalah topik yang baru-baru ini telah muncul dalam literatur penelitian. Masalah utama adalah bagaimana sering, efisien dan aman memverifikasi bahwa server penyimpanan dapat menyimpan kliennya pada Data outsourcing (berpotensi sangat besar). Server penyimpanan diasumsikan baik dari segi keamanan dan keandalannya. Masalah ini menjadi perangkat komputasi kecil dengan sumber daya yang terbatas. Saat klien mengirmkan request untuk memproses data yang telah disimpannya di cloud, algoritma privacy manager akan menyusun kembali data yang telah telah dipisah tersebut untuk ditampilkan lagi secara utuh di sisi klien. ada saat proses transmisi data tersebut, resiko data ada yang hilang atau rusak diperjalanan tetap selalu ada. Untuk mengatasi hal tersebut, algoritma privacy manager menggunakan risk manager untuk menghitung jumlah atau besar ukuran suatu data. Sehingga jika besar ukuran

data yang telah disusun tersebut tidak sesuai dengan ukuran awal, sistem secara otomatis akan meminta cloud server untuk mengirim ulang paket yang hilang.

Pada paper Provable Data Possession at Untrusted Stores tahun 2007 oleh Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, Dawn Song, kepemilikan data yang dapat dibuktikan (PDP) yang memungkinkan klien yang telah disimpan data pada server terpercaya untuk memverifikasi bahwa server memiliki data asli tanpa mengambilnya. Model ini menghasilkan probabilistik kepemilikan dengan blok dari server. Pada paper ini menyajikan dua skema PDP provably yang aman dan lebih efisien. bahkan jika dibandingkan dengan skema yang mencapai jaminan lemah. privacy manager, untuk data yang memiliki large size key word akan diproses di dalam privacy manager. Keywords ini disimpan di dalam database privacy manager itu sendiri untuk nantinya didekripsi kembali saat dikembalikan kepada klien. Keyword tersebut tidak hanya bisa dihasilkan oleh privacy manager, tetapi juga oleh klien itu sendiri Algoritma generate keyword yang digunakan adalah algoritma RSA.

Pada paper ini fokus pada masalah memverifikasi jika server tidak terpercaya yang menyimpan data pada klien. Dan juga memperkenalkan karena memiliki data yang dapat dibuktikan, di mana yang dapat diinginkan untuk meminimalkan blok berkas mengakses, perhitungan di server, dan komunikasi client-server. Solusi untuk PDP sangat cocok digunakan pada metode ini. Mereka memungkinkan untuk memverifikasi kepemilikan data tanpa memiliki akses ke file data aktual.

Jadi, keamanan dan privasi menjadi hal yang utama di dalam teknologi cloud computing saat ini. Penggunaan resource secara bersama berdampak dengan rentannya suatu data dan informasi tersebut bocor dan disalahgunakan oleh pihak lain yang tidak seharusnya memiliki informasi tersebut. Ancaman privasi data dapat berasal dari pihak internal (penyedia layanan, pengguna dalam perusahaan), dan kebocoran data bisa terjadi karena kegagalan hak akses keamanan di beberapa domain.