BAB 2
Tinjauan Pustaka

2.1 Penelitian Terdahulu

Bukti dalam hal ini adalah bukti digital merupakan hal yang sangat penting dalam menunjang penyelidikan suatu kasus. Namun, bukti digital khususnya harus dianggap skeptis karena hanya ada dalam representasi biner. Tanpa mekanisme perlindungan yang memadai, data tersebut dapat dengan mudah dimanipulasi tanpa meninggalkan jejak. Pengumpulan, penanganan, penyimpanan dan penyajian bukti digital telah menemui beberapa masalah di masa lalu (Richter, Kuntze, & Rudolph, 2010). Richter et al. (2010) sendiri melakukan penelitian membuat sistem pengukuran dalam mengumpulkan barang bukti digital dalam hal ini adalah pelanggaran lalu lintas. Richter et al. menekankan bahwa dalam membuat sistem pengukuran dalam mengumpulkan barang bukti digital, forensik data digital harus digunakan selama proses rekayasa sistem. Selain itu, dalam perencanaan sistem diperlukan konsep pengambilan keputusan yang matang agar sistem memiliki tingkat reliabitas dan keamanan yang tinggi. Namun, mengenai penyimpanan bukti digital belum banyak penelitian yang membahas mengenai tempat penyimpanan barang bukti digital yang memadai.

Davis et al. (2005) telah membangun Arsitektur *Digital Evidence Custodian* (DEC) *network-based* dengan kemampuan penyimpanan data yang besar menggunakan teknologi *storage area network* (SAN) dan *network-attached storage* (NAS). Arsitektur DEC yang dibangun oleh Davis dikatakan sebagai solusi penyimpanan *digital evidence* berbasis *network* yang kuat, namun relatif murah, untuk menyimpan dan menangani sejumlah besar bukti digital. Dalam penelitian tersebut, *Digital Evidence* Storage *Locker* (DESL) yang dibangun tersebut dapat memfasilitasi pemrosesan kolaboratif bukti digital oleh penguji, penyelidik dan agen kasus yang mungkin berada di lokasi berbeda. Selain menyederhanakan tugas dalam hal menyimpan bukti dan mempertahankan integritasnya, arsitektur DEC berbasis *network* secara signifikan meningkatkan produktivitas penyelidikan forensik digital dengan mendukung akses terdistribusi dan pemrosesan bukti digital.

Ali et al. (2019) membuat sistem Chain of Custodian Reflex (COC Reflex yang menggunakan teknologi SAN sebagai konsep arsitektur penyimpanan terpusat berbasis jaringan dan teknologi berbasis web. Sistem COC Reflex yang dibangunnya memberikan alternatif penyimpanan bukti digital yang tidak bergantung pada penyimpanan internal dan

sistem akses yang tidak bergantung pada satu perangkat saja. Konsep COC reflex juga mendukung upaya kolaborasi antar petugas dalam menangani bukti digital yang dikelola, karena bukti digital yang dikelola disimpan dalam penyimpanan eksternal berbasis *cloud*.

Paul Chinnaraju et al. (2018) dalam papernya membandingkan penyimpanan traditional seperti SAN, NAS dll dengan *Software Defined Strorage* (SDS) dari perspektif *storage vendor*. Kriteria yang dibahas dalam paper tersebut meliputi aspek biaya, kelincahan (*agility*), skalabilitas, reliabilitas, dan multi-tenancy. Hasilnya, dengan kriteria seperti biaya, kelincahan, skalabilitas, reliabilitas, dan multi tenancy menjadikan SDS lebih baik daripada penyimpanan lama. Dalam hal skalabilitas, penyimpanan tradisional hanya dapat diskalakan hingga maksimal 4 – 8 *controller*, sedangkan SDS dapat menskalakan hingga ratusan ribu node - yang artinya secara teoritis dapat diskalakan tanpa batas.

Kaitannya dengan SDS, Weil (2006) telah mengembangkan Ceph yaitu salah satu SDS yang memberikan performa, reliabilitas, dan skalabilitas yang luar biasa. Weil menyebut Ceph sebagai sistem file terdistribusi yang memaksimalkan pemisahan antara manajemen data dan metadata dengan mengganti tabel alokasi dengan fungsi distribusi data pseudo-random yang dirancang untuk kluster heterogen dan dinamis dari *Object Storage Devices* (OSD) yang tidak dapat diandalkan. Fitur tersebut didukung oleh RADOS (*Reliable Autonomic Distributed Object Storage*) sebagai inti pengembangan Ceph. RADOS meningkatkan kecerdasan perangkat dengan mendistribusikan replikasi data, deteksi kegagalan, dan pemulihan ke OSD semi-otonom yang menjalankan sistem file objek lokal. *Cluster* metadata terdistribusi dinamis menyediakan manajemen metadata yang sangat efisien dan secara mulus beradaptasi dengan berbagai tujuan umum dan beban kerja sistem komputasi file ilmiah (Weil et al., 2006).

Mengenai performa Ceph dalam hal skabilitas telah diuji oleh Wang et al. (2013). Wang et al. mengevaluasi file dan memblokir kinerja I / O dan skalabilitas Ceph, menggunakan sistem penyimpanan *highend* komersial. Wang berhasil meningkatkan kinerja RADOS hingga 16,3%. Setelah penyetelan berulang, sistem Ceph Wang mampu mencapai 70% kemampuan perangkat keras mentah di tingkat RADOS, dan 62% di tingkat filesystem. (Wang et al., 2013).

Selain Wang, penelitian mengenai skalabilitas Ceph juga dilakukan oleh Gudu, Hardt, & Streit (2015) dengan menambahkan OSD pada sistem berjalan hingga berjumlah 20 OSD (10 node). Dari penelitian yang dilakukan Gudu tersebut, kinerja Ceph meningkat secara stabil seiring dengan penambahan jumlah OSD.

Ceph juga telah banyak diimplementasikan untuk membantu pengelolaan dan pertukaran data menggunakan *Software Defines Networking* (SDN) yang tidak memerlukan perangkat khusus pada sistem *storage*, salah satunya adalah OSIRIS (McKee et al., 2017). OSIRIS merupakan sistem *storage* yang dibangun untuk menjembatani peneliti dari empat universitas di US untuk mengkolaborasikan data dengan mudah tanpa membangun infrastruktur sendiri. Peneliti di setiap kampus dapat membaca, menulis, mengelola, dan berbagi data langsung dari lokasi komputasi mereka sendiri.

Penelitian-penelitian tersebut diringkas ke dalam Tabel 2.1.

Tabel 2.1 Penelitian terdahulu

Peneliti	**Topik Penelitian**	**Hasil Penelitian**
(Richter et al., 2010)	Membuat sistem pengukuran untuk pengumpulan bukti digital dalam kasus pelanggaran lalu lintas sehingga bukti digital tidak dapat disangkal kebenaraannya.	Dalam perencanaan sistem diperlukan konsep pengambilan keputusan yang matang agar sistem memiliki tingkat reliabitas dan keamanan yang tinggi.
(Davis et al., 2005)	Membangun penyimpanan barang bukti digital berbasis jaringan (*network-based*) menggunakan teknologi NAS dan SAN	Arsitektur DEC yang dibangun secara signifikan meningkatkan produktivitas penyelidikan forensic digital dengan mendukung akses terdistribusi dan pemrosesan digital.
(Ali et al., 2019)	Membangun sistem repositori *network – based* untuk penyimpanan barang bukti digital dengan menggunakan teknologi SAN dan berbasis web.	Sistem yang dibangun menawarkan kemudahan akses secara fleksibel dan efektif serta memungkinkan kolaborasi antar petugas dalam menangani bukti digital yang dikelola.
(Paul Chinnaraju et al., 2018)	Membandingkan penyimpanan traditional seperti SAN, NAS dll dengan *Software Defined Strorage* (SDS) dari perspektif *storage vendor*.	SDS lebih unggul dibandingkan sistem penyimpanan lama (NAS, SAN dll) dari aspek biaya, agilitas, skalabilitas, reliabilitas, dan multi tenancy.
(S. A. Weil et al., 2006)	Mengembangkan Ceph, sebuah SDS dengan RADOS sebagai landasannya yang memungkinkan pemisahan manajemen data dan metadata, mendistribusikan replikasi data, deteksi kegagalan, dan pemulihan ke	Ceph mengatasi tiga tantangan kritis sistem penyimpanan — skalabilitas, kinerja, dan reliabilitas.

Peneliti	Topik Penelitian	Hasil Penelitian
	OSD semi-otonom yang menjalankan sistem file objek local.	
(Wang et al., 2013)	Menguji kemampuan Ceph dalam hal skalabilitas	Kemampuan Ceph dapat ditingkatkan hingga hampir 70% kemampuan perangkat keras mentah pada tingkat RADOS dan mendekati 62% pada tingkat sistem file.
(Gudu et al., 2015)	Menguji skalabilitas Ceph salah satunya dengan menambahkan OSD pada sistem berjalan hingga berjumlah 20 OSD (10 node).	Kinerja Ceph meningkat secara stabil seiring dengan penambahan jumlah OSD
(McKee et al., 2017)	Menggunakan Ceph untuk membangun OSiRIS, sebuah sistem *storage* yang menjembatani peneliti dari beberapa kampus di US untuk dapat mengkolaborasikan data tanpa harus membangun infrastruktur sendiri.	OSiRIS yang dibangun dengan Ceph memungkinkan peneliti di setiap kampus dapat membaca, menulis, mengelola, dan berbagi data langsung dari lokasi komputasi mereka sendiri.
Penelitian yang akan dilakukan	Membangun tempat penyimpanan barang bukti menggunakan *software – defined storage* Ceph yang memenuhi kriteria dari aspek *scalability*, *confidentiality*, *integrity* dan *availability*.	

2.2 Landasan Teori

2.2.1 Barang Bukti Digital

Barang bukti merupakan hal yang paling penting dalam membuktikan sebuah kejahatan. Dalam kejahatan siber (*cyber crime*) dan kejahatan yang melibatkan perangkat elektronik umumnya, barang bukti yang dapat digunakan adalah bukti fisik / perangkat keras dan juga bukti-bukti digital. Beberapa ahli mendefinisikan bukti digital sebagai berikut:

- Bukti digital didefinisikan sebagai informasi yang didapat dalam bentuk/format digital (Scientific Working Group on Digital Evidence, 1999), baik berupa bukti yang riil maupun abstrak (perlu diolah terlebih dahulu sebelum menjadi bukti yang riil).
- Bukti digital adalah objek digital yang berisi informasi andal yang mendukung atau membantah hipotesis (Carrier, 2005).

- Bukti digital didefinisikan sebagai data yang disimpan atau dikirimkan menggunakan komputer yang digunakan untuk mendukung atau menyangkal teori tentang bagaimana suatu pelanggaran terjadi atau elemen-elemen penting dari pelanggaran tersebut. Data yang dimaksud kombinasi dasar dari angka-angka yang merepresentasikan dari berbagai jenis informasi seperti teks, gambar, audio, dan video (Casey, 2011).
- Dalam situs National Institute of Justice (www.nij.gov), pengertian bukti digital yaitu informasi yang disimpan atau ditransmisikan dalam bentuk biner yang dapat diandalkan di pengadilan. Bukti digital tersebut dapat ditemukan pada hard drive komputer, ponsel, *personal digital assistant* (PDA), CD, dan kartu flash di kamera digital, dan tempat-tempat lainnya (National Institute of Justice, 2016).

Jika kita melihat dari beberapa definisi yang diutarakan oleh pakar, maka kita dapat mengambil kesimpulan bahwa bukti digital adalah informasi yang tersimpan atau terdistribusikan dalam komputer atau dalam bentuk digital yang bisa dijadikan sebagai bukti dalam persidangan. Informasi tersebut dapat berupa text, gambar, audio, video yang bisa kita temukan pada harddrive computer, ponsel atau smartphone, CD/DVD, kartu flash/memory dan lainnya.

Hukum di Indonesia telah mengakui bukti digital sebagai alat bukti yang sah di persidangan melalui Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yaitu dalam Pasal 5 ayat (1) dan ayat (2) UU ITE yang menyebutkan:

> 1. *Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.*
> 2. *Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.*

Lebih lanjut, untuk dapat diakui sebagai alat bukti yang sah pasal 6 UU ITE menyebutkan :

> *"Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya* ***dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggung jawabkan sehingga menerangkan suatu keadaan."***

2.2.2 Karakteristik Barang Bukti Digital

Menurut Richter, Kuntze, & Rudolph, (2010) untuk dapat diterima di persidangan barang bukti digital harus memenuhi karakteristik bukti digital yaitu *Admissible* (layak), *Authentic* (asli), *Complete* (lengkap), *Reliable* (dapat dipercaya) dan *Believable* (terpercaya).

- ***Admissible***

  Barang bukti digital harus sesuai dengan fakta dan masalah yang terjadi dan dapat diterima serta digunakan secara hukum mulai dari proses penyidikan sampai ke pengadilan.

- ***Authentic***

  Bahwa barang bukti harus mempunyai hubungan keterkaitan yang jelas secara hukum dengan kasus yang diselidiki dan barang bukti bukan hasil rekayasa. Selain itu, barang bukti digital harus dapat dibuktikan dalam pengadilan bahwa barang bukti tersebut masih asli dan tidak pernah diubah-ubah..

- ***Complete***

  Barang bukti harus lengkap dan dapat membuktikan tindakan jahat yang dilakukan pelaku kejahatan. Barang bukti yang dikumpulkan, tidak cukup hanya berdasarkan satu perspektif dari sebuah kejadian yang berlangsung.

- ***Reliable***

  Barang bukti yang dikumpulkan harus dapat dipercayai. Pengumpulan barang bukti dan analisis yang dilakukan harus sesuai prosedur dan dilakukan dengan jujur. Selain itu barang bukti tidak boleh meragukan dan benar benar harus dapat dipercayai serta sesuai dengan prosedur yang SOP yang berlaku.

- ***Believable***

  Barang bukti dan presentasi yang dilakukan di pengadilan harus dapat dimengerti oleh hakim dan dapat dipercayai. Penyampaian barang bukti di pengadilan harus menggunakan bahasa awam yang dapat dimengerti oleh hakim.

2.2.3 Penyimpanan Bukti Digital

Setelah barang bukti diakuisisi, selajutnya barang bukti disimpan untuk dapat dilakukan penyidikan lebih lanjut. Penyimpanan bukti digital termasuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Bukti harus benar-benar steril artinya belum mengalami proses apapun ketika diserahkan kepada ahli digital forensik

untuk diteliti. Hal ini dapat dijamin dengan *chain of custody* (rantai barang bukti), yaitu kronologis pendokumentasian barang bukti. *Chain of custody* akan mendokumentasikan hal terkait dengan *where*, *when*, *why*, *who* and *how* dari penggunaan barang bukti pada setiap proses investigasi. Lingkup dari chain of custody meliputi semua individu yang terlibat dalam proses akuisisi, koleksi, analisis bukti, catatan waktu serta informasi kontekstual meliputi labelling kasus, unit dan laboratorium yang memproes barang bukti (Prayudi, 2014).

Sementara itu, karena bukti digital bersifat sementara (*volatile*), mudah rusak, berubah dan hilang, maka penanganan pemrosesan bukti digital harus benar-benar diperhatikan. Kesalahan kecil pada penanganan bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan. Bahkan menghidupkan dan mematikan komputer dengan tidak hati-hati bisa saja merusak/merubah barang bukti tersebut.

Aturan utama pada tahap ini adalah penyelidikan tidak boleh dilakukan langsung pada bukti asli karena dikhawatirkan akan dapat merubah isi dan struktur yang ada didalamnya. Mengantisipasi hal ini maka dilakukan *copy* data secara Bitstream image dari bukti asli ke media penyimpanan lainnya (Shinder & Cross, 2008). Bitstream image adalah metode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk file yang tersembunyi (*hidden files*), file temporer (*temporary file*), file yang ter-*defrag* (*defragmented file*), dan file yang belum ter-*overwrite*. Dengan kata lain, setiap biner digit demi digit di-*copy* secara utuh dalam media baru. Teknik ini umumnya diistilahkan dengan *cloning* atau *imaging*. Hasil *cloning* disimpan dalam suatu tempat penyimpanan barang bukti digital (*digital evidence storage*) di Laboratorium Forensik untuk selanjutnya dapat dilakukan pemeriksaan, dan penyelidikan.

Digital evidence storage merupakan infrastruktur penting yang mendukung proses penyimpanan bukti digital. Untuk menjaga agar barang bukti diterima di persidangan, sistem *digital evidence storage* harus memenuhi kriteria keamanan informasi berupa *Confidentiality*, *Integrity* dan *Availability*.

2.2.4 Clustered Storage

Suatu *cluster* adalah suatu kelompok dua atau lebih *server* yang didedikasikan khusus untuk menjalankan suatu aplikasi atau beberapa aplikasi.

Sedangkan yang dimaksud *storage cluster* atau *clustered storage* adalah jaringan beberapa sistem *storage* yang berperilaku sebagai satu sistem yang bekerja sama untuk

meningkatkan kinerja, kapasitas serta reliabilitas sistem. Dalam arti yang paling abstrak, *storage cluster* terdiri dari beberapa server *storage* yang dapat diakses melalui jaringan, biasanya dengan memasang sebagai virtual *filesystem* di dalam *server*. Fitur biasanya mencakup tingkat redundansi dan ketersediaan yang tinggi. Misalnya jika satu server di *cluster* penyimpanan mengalami kegagalan, data masih dapat diakses dari server lain dalam *cluster* itu. Selain ketersediaan data dan kemudahan akses, manfaat lain yang ingin dicapai dari penggunaan sebuah *storage cluster* adalah kemudahan penambahan kapasitas.

Setiap sistem dalam sebuah cluster disebut node. Setiap node adalah sistem nyata dan lengkap dengan semua sumber daya yang dibutuhkan seperti prosesor, memori, perangkat I/O, dan sub sistem penyimpanan yang bekerja di bawah kendali salinan sistem operasinya sendiri.

Beberapa keuntungan penggunaan metode *clustering* seperti yang diutarakan oleh Chevance (2005) adalah :

- Tingkat availabilitas yang tinggi
- Implementasi perangkat keras sederhana
- Kompatibilitas sampai tingkat aplikasi dengan uniprocessor maupun multiprosesor
- Peningkatan kinerja
- Integrasi teknologi baru yang mudah (versi prosesor dan OS)
- Kemudahan dalam hal *maintenance*.

2.2.5 Software Defined Storage

Software defined storage (SDS) adalah istilah untuk *software* penyimpanan data komputer yang memungkinkan pengelolaan penyimpanan data yang pembuatan dan pengelolaannya terlepas dari keterikatan terhadap perangkat keras yang mendasarinya. *Software defined storage* biasanya mencakup bentuk virtualisasi *storage* untuk memisahkan *storage hardware* dari *software* yang mengelolanya. Perangkat lunak ini menyediakan kebijakan manajemen untuk bermacam pilihan fitur, seperti deduplikasi data, replikasi, *thin provisioning*, *snapshot* dan backup.

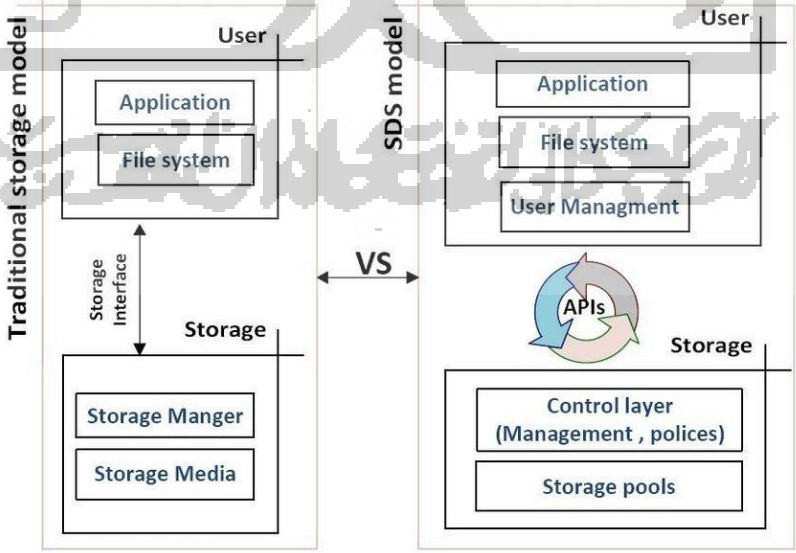
Transisi ke *storage* virtual ini membuka masa depan tempat penyimpanan termasuk kemampuan untuk meningkatkan skalabilitas dengan mudah. SDS menghapus batasan penguncian *vendor* dari pendekatan penyimpanan tradisional, dan, sebagai standar

pemrograman aplikasi (API), harus memungkinkan *mashup* berbagai layanan *vendor* untuk mencapai set fitur yang diinginkan (O'Reilly, 2017).

Carlson et al., (2015) mendefinisikan SDS secara umum harus mencakup :

- Otomasi - Manajemen sederhana yang mengurangi biaya pemeliharaan infrastruktur penyimpanan.
- Antarmuka Standar - API untuk manajemen, penyediaan, dan pemeliharaan perangkat dan layanan penyimpanan.
- Jalur Data Virtual - antarmuka Blok, File dan Objek yang mendukung aplikasi yang ditulis ke *interface* ini.
- Skalabilitas - Kemampuan untuk meningkatkan skalabilitas penyimpanan tanpa mengganggu ketersediaan atau kinerja.
- Transparansi - Kemampuan bagi konsumen *storage* untuk memantau dan mengelola kebutuhan penyimpanan mereka sendiri sesuai dengan sumber daya dan biaya yang tersedia.

Salah satu masalah terpenting dalam merancang sistem penyimpanan data adalah memastikan bahwa persyaratan *quality of services* (QoS) aplikasi berhasil diterapkan. Teknologi penyimpanan tradisional tidak mendukung persyaratan ini secara efisien. Selain itu, otomatisasi dan adaptasi terhadap perubahan dalam lingkungan yang dinamis terbatas pada teknologi saat ini. Semua masalah ini dapat diselesaikan oleh SDS. Perbandingan antara model penyimpanan tradisional dan model SDS disajikan pada Gambar 2.1.



Gambar 2.1 Perbandingan antara model penyimpanan tradisional dan model SDS

Perhatikan bahwa, dalam model penyimpanan tradisional, *interface* digunakan untuk menginterpretasikan berbagai permintaan *user* ke media penyimpanan, dan *interface* ini harus diubah ketika tipe data dalam media penyimpanan diubah (mis. objek, file, dll.). Sebaliknya desain SDS memiliki lapisan kontrol untuk menetapkan kebijakan yang berbeda untuk menanggapi berbagai permintaan dari *end-user* melalui API (Darabseh et al., 2015).

Paul Chinnaraju et al. (2018) membandingkan penyimpanan tradisional seperti SAN dan NAS dengan *Software Defined Storage* dilihat dari sisi vendor penyedia *storage* / *Data Center*. Hasilnya, *Software Defined Data Center* (SDDC) dan jaringan pendukungnya dengan kriteria seperti biaya, agilitas, skalabilitas, dan keandalan adalah sistem yang yang lebih baik daripada sistem penyimpanan tradisional.

- Biaya: Penyimpanan tradisional seperti NAS dan SAN masih menghabiskan lebih banyak biaya untuk operasionalnya.
- *Agility*: secara umum, *agility* berarti melakukan beberapa pekerjaan lebih cepat, dan jauh lebih cepat. Faktor penting untuk dipertimbangkan dalam hal *agility* adalah otomasi kerja sampai selesai. Penyimpanan tradisional menggunakan *Command Line Interfaces* (CLI) atau API spesifikasi inisiatif manajemen penyimpanan untuk mengotomatisasi semua operasinya. Tetapi SDS menggunakan REST API yang lebih sederhana untuk mengotomatisasi semua pekerjaannya
- Skalabilitas: Skalabilitas didefinisikan sebagai kemampuan untuk memperbesar infrastruktur penyimpanan tanpa menghambat kinerja. SDS dapat memiliki ratusan *node*, atau ribuan *node* yang terhubung ke jaringan standar. Hal ini memberikan fitur bahwa jumlah *drive* yang dapat dihubungkan dengan *controller* adalah tidak terbatas. Dengan SDS, *user* dapat meningkatkan kapasitas penyimpanan hampir secara instan, sehingga menjadikannya hemat biaya serta fleksibel dan dapat diskalakan dengan mudah.
- *Reliability*: SDS tergantung terutama pada *software*-nya untuk keandalan data yang disimpan, dengan asumsi bahwa ada lebih banyak peluang bagi *hardware* untuk mengalami kegagalan jika infrastruktur sangat skalabel. Kecerdasan, proses *self-reconstructing* dari *software* ini menjamin kerja yang berkelanjutan dari segala sesuatu di lingkungan itu. Fitur-fitur penyimpanan yang ditentukan oleh SDS membuatnya lebih andal dari pada sistem penyimpanan tradisional. Pendekatan melalui jaringan ini telah menjadikan internet dan berbagai protokolnya lebih andal. Dengan cara yang sama, TCP

/ IP akan memastikan bahwa jika ada kegagalan saat mentransfer paket antara dua node, dengan kecerdasannya ia harus mengubah rute paket melalui rute alternatif untuk memastikan keandalan data.