KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA

Zen Munawar, S.T.,M.Kom[1] , Novianti Indah Putri,S.T[2]

1. Manajemen Informatika, Politeknik LP3I Bandung
2. Teknik Informatika, Fakultas Teknologi Informasi Universitas Bale Bandung

ABSTRACT

When life is more comfortable than in the past, because of the development of computers with the internet that has contributed to the comfort of human life. However, it is realized or not the potential dangers behind the convenience of using the internet. In our real world everyday some of us do not know of the many potential safety hazards where computers are connected to the internet this is because most use computers in relatively small areas, such as families, workplaces or in the school / campus environment. If we use it on a large scale, a number of problems will emerge, in this study we will discuss the forms and factors of computer security threats, as well as some suggestions for improving the prevention of computer security threats. After understanding the factors that threat to computer security, the next step is to discuss preventive measures against computer threats as a contribution of computer development in the future.

Key Word: Security, computer networks, prevention of computer threats.

ABSTRAK

Pada saat kehidupan lebih nyaman dibandingkan masa lalu, karena dengan adanya perkembangan komputer dengan internetnya yang telah memberikan kontribusi dalam kenyamanan hidup manusia. Namun demikian disadari atau tidak adanya potensi bahaya dibalik kenyamanan penggunaan internet. Di Dunia nyata kita sehari-hari beberapa dari kita tidak tahu akan banyaknya potensi bahaya keamanan dimana komputer terhubung dengan internet hal ini karena kebanyakan menggunakan komputer dalam area yang relative kecil, seperti keluarga, tempat bekerja atau di lingkungan sekolah / kampus. Jika kita menggunakan pada skala besar maka akan muncul beberapa masalah, dalam penelitian ini akan membahas bentuk dan faktor ancaman keamanan komputer, juga beberapa saran untuk meningkatkan pencegahan dari ancaman keamanan komputer. Setelah memahami faktor yang ancaman keamanan komputer, selanjutnya dibahas tindakan pencegahan terhadap ancaman komputer sebagai kontribusi dari perkembangan komputer di masa yang akan datang.

Kata Kunci: Keamanan, jaringan komputer, pencegahan ancaman komputer

1. PENDAHULUAN

Pada bagian ini akan di bahas tinjauan keamanan lingkungan jaringan komputer, pengguna komputer sangat menyadari bahwa kenyamanan penggunaan komputer dalam kehidupan kita sehari-hari adalah hal yang paling dasar, karena fungsinya seperti otomatisasi, kedirgantaraan, kedokteran dan kesehatan, penelitian ilmiah, investigasi kriminal dan sebagainya, komputer memiliki peran penting yang tidak tergantikan. Terdapat banyak informasi dalam industri yang sifatnya sangat rahasia, karena ini informasi tidak dapat dipahami oleh orang yang tidak relevan, jika tidak maka akan menyebabkan kerugian yang tidak dapat diperbaiki. Tepatnya karena tingginya rahasia informasi komputer sehingga beberapa orang yang berniat jahat memiliki ide untuk melakukan kejahatan dan selalu berharap untuk mendapatkan beberapa manfaat dari kerentanan keamanan jaringan komputer. Jaringan komputer teknologi keamanan terus berkembang, dan teknologi kriminal dari para penjahat ini juga terus menerus berkembang.

Bahkan beberapa teknologi kriminal lebih tinggi dari level ahli komputer, sehingga jaringan keamanan tidak bisa dijamin. Karena bukti dalam proses kejahatan komputer sulit untuk dipahami, komputer kejahatan keamanan jaringan semakin sering terjadi. Ada hal penting yang perlu dilakukan yaitu melakukan pekerjaan dengan baik dalam pencegahan keamanan jaringan komputer, untuk meminimalkan kemungkinan terjadinya kejahatan komputer.

Keamanan jaringan komputer tidak terdiri dari satu aspek, tetapi mengandung empat tautan penting: perangkat lunak, perangkat keras jaringan, layanan Internet of Things dan sumber daya bersama. Menurut definisi komputer keamanan jaringan oleh Organisasi Internasional untuk Standardisasi, keamanan jaringan komputer mengacu pada perlindungan perangkat keras, perangkat lunak, dan sumber daya data dalam sistem komputer agar tidak dihancurkan, diubah, atau lubang keamanan karena

alasan kecelakaan atau berbahaya, sehingga sistem komputer terus beroperasi dengan handal, serta layanan komputer

juga teratur. Untuk suatu sistem, peralatan fisik seperti sirkuit perangkat keras harus digunakan sebagai carrier, maka program fungsional pada carrier dapat dijalankan. Dengan menggunakan perangkat jaringan seperti router, hub, switch dan kabel, pengguna dapat membangun jaringan komunikasi yang mereka butuhkan. Untuk jaringan area lokal nirkabel skala kecil, orang dapat menggunakan perangkat ini untuk membangun jaringan komunikasi yang mereka butuhkan. Cara paling sederhana untuk melindungi mereka adalah dengan mengatur instruksi yang sesuai pada router nirkabel untuk mencegah pengguna ilegal dari pengganggu [1]. Sebagai perlindungan protokol komunikasi, protokol enkripsi WPA2 yang banyak digunakan untuk protokol enkripsi. Pengguna dapat mengakses router hanya dengan menggunakan kunci. Biasanya, driver dapat dianggap sebagai bagian dari sistem operasi. Setelah mendaftar dengan registry, antarmuka driver komunikasi jaringan yang sesuai dapat dipanggil oleh program aplikasi komunikasi.

Saat ini, sejumlah besar data yang dikumpulkan dan dihasilkan setiap hari menawarkan berbagai peluang analitis bagi organisasi untuk mengungkap informasi yang bermanfaat untuk operasinya. Jumlah data yang sangat besar dan jumlahnya banyak kemungkinan analitis menyebabkan lahirnya istilah 'data besar'. Data besar seringkali ditentukan oleh karakteristiknya - "3V" yang mewakili volume, variasi, dan kecepatan data [2]. Beberapa ilmuwan sarjana juga telah memperkenalkan "V" keempat yang kebenaran data [3]. Organisasi dihadapkan dengan lingkungan pasar badai saat ini secara konsisten mencari untuk mengadopsi teknologi canggih yang dapat membantu dalam mendapatkan keunggulan kompetitif dan membangun kemampuan inovatif. Pengenalan teknologi *big data* dapat menawarkan organisasi dengan solusi yang dibutuhkan, dengan memberikan kemampuan untuk menganalisis volume data yang lebih besar dengan kecepatan dan akurasi yang lebih besar dari yang sebelumnya mungkin. Aplikasi dan perananya sekarang dikenal luas tidak hanya dalam bisnis, tetapi juga di sektor lain seperti layanan kesehatan dan pemerintah, meliputi berbagai disiplin ilmu.

Namun, sebelum memutuskan untuk mengadopsi solusi *big data*, ada beberapa keputusan awal dan langkah-langkah itu harus dipertimbangkan oleh organisasi. Selain masalah awal seperti keuntungan relatif, biaya dan teknis keahlian, satu masalah kritis lain yang harus dipertimbangkan oleh organisasi yang memutuskan untuk mengadopsi solusi *big data* adalah masalah keamanan dan privasi [4]. Dengan jatuh tempo solusi *big data*, keamanan dan privasi menghadirkan keprihatinan serius bagi berbagai pihak; perorangan, organisasi dan pemerintah, terutama karena banyaknya data pribadi yang dikumpulkan dan dianalisis. Selama proses adopsi teknologi, merupakan hal biasa bagi sebuah organisasi untuk menemukan keamanan baru

ancaman dan tantangan yang ditimbulkan oleh teknologi. Kejadian yang sama harus diharapkan dalam adopsi BDS. Namun, keamanan sering diperlakukan sebagai renungan di sebagian besar organisasi. Ini dapat menyebabkan kegagalan keamanan terutama karena disebabkan oleh penggunaan metode deteksi ancaman yang tidak tepat dan mekanisme keamanan dalam perlindungan data [5]. Untuk organisasi dengan lingkungan data besar, keamanan tidak boleh diperlakukan sebagai sekunder, sehingga sangat ideal untuk diberikan mekanisme keamanan dari bawah ke atas bukannya "menambahkan keamanan ke lingkungan data yang sudah kompleks sebagai renungan "[6]. Organisasi dengan mekanisme keamanan dan privasi yang mapan dalam pengembangan dan penggunaan big data akan menuai hasil yang lebih diinginkan dan lebih sedikit pushback konsumen [7].

2 KAJIAN TEORITIS

Bagian ini membahas peran dan pentingnya kemanan komputer dilihat dari berbagai aspek baik perangkat lunak maupun perangkat keras.

2.1 Bentuk Ancaman Keamanan jaringan Komputer

Keamanan jaringan komputer melibatkan empat hubungan yang berbeda, yaitu potensi hubungan dengan empat aspek utama ketika menggambarkan bentuk-bentuk ancaman terhadap keamanan jaringan komputer. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer: penyalahgunaan informasi Internet of Things, penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi komputer. Pertama Kesalahan Informasi Internet of Things, Biasanya, dalam proses menggunakan komputer, banyak pengguna lebih tenang saat mengklik situs web dan mengunduh gambar, file, dan sebagainya, dan tidak akan digunakan setelah pemakaian. Hal ini akan menyebabkan bahaya besar yang tersembunyi pada keamanan jaringan komputer, karena setiap situs web, file, tautan dan sebagainya sangat mungkin mengandung virus atau ada file yang disembunyikan serta hal lainnya yan berbahaya, jika tidak ada aplikasi untuk menyaring virus atau file yang tersembunyi, maka dapat menyebabkan kebocoran informasi atau infeksi terhadap komputer. Kedua serangan pada layanan latar belakang, serangan latar belakang berupa penolakan layanan yang disebut adalah bahwa pengguna sengaja menunda atau secara ilegal menunda layanan jaringan dalam proses mengunjungi situs web atau mengunduh file seperti biasa, sehingga menyebabkan kerusakan tertentu pada keamanan jaringan komputer. Ketiga kehancuran integritas keamanan jaringan komputer, peretas atau orang lain yang tidak mematuhi kode etik dengan sengaja menggunakan berbagai cara ilegal untuk menghancurkan keamanan jaringan komputer, sehingga memengaruhi integritas keamanan komputer. Keempat memberitahukan informasi komputer, ketika informasi dalam jaringan komputer ditransmisikan secara langsung ke entitas yang tidak sah tanpa izin dari pengguna, maka sudah pasti informasi menjadi rentan.. Bentuk umum dari informasi komputer yang rentan karena ada lubang tersebut termasuk aspek-aspek berikut: intrusi virus atau Trojan horse ke komputer, kerentanan sistem pengguna sendiri, penyadapan frekuensi gelombang radio pada informasi komputer, pemasangan peralatan pemantauan, pengamanan jaringan komputer.

2.2 Faktor-Faktor Yang mengancam Kemanan Jaringan Komputer

Ada banyak faktor yang mengancam keamanan jaringan komputer, yang dapat dibagi menjadi faktor subyektif dan faktor obyektif. Untuk menggambarkan faktor-faktor yang mengancam keamanan jaringan komputer agar lebih komprehensif.

a. Spam dan Spyware

Dalam bentuk komunikasi yang biasa, berkirim email adalah cara yang lebih umum digunakan. Terutama di semua jenis pekerjaan seringkali, email memainkan peran yang sangat penting dalam melakukan pekerjaan. Karena alasan ini, maka banyak penjahat ingin menggunakan email untuk mencuri privasi pengguna atau ada tujuan lain. Mereka terutama memaksa pengguna untuk menerima spam dengan memasukkannya ke dalam email yang mereka kirimkan. Jika pengguna tidak memperhatikan validitas email ini, mereka dapat mengklik atau mengunduh perangkat lunak khusus yang mereka masukkan, maka akan terjadi kehilangan informasi.

b. Serangan dan Ancaman Hacker

Peretas merujuk pada sekelompok orang dengan kecerdasan dan kemampuan tinggi, yang akrab dengan pengetahuan komputer dan sangat pandai dalam keamanan jaringan komputer [8].

Dibandingkan dengan orang biasa, peretas menunjukkan ketakutan kepada pengguna. Peretas dapat memilih serangan destruktif dan serangan non-destruktif jika ingin memenuhi kebutuhan mereka sendiri melalui jaringan komputer. Serangan destruktif, seperti menghancurkan sistem pengguna sehingga komputer benar-benar tidak dapat digunakan. Serangan non-destruktif berarti peretas hanya mengambil informasi yang mereka butuhkan tanpa mempengaruhi penggunaan normal pengguna. Peretas umum menggunakan cara serangan: serangan kuda Trojan, serangan phising terhadap situs web, serangan email dan sebagainya.

c. Implantasi virus

Pengguna komputer takut terhadap virus komputer, karena virus dapat disisipkan ke berbagai jenis aplikasi program, pengguna dengan tidak sengaja akan mengklik virus tersebut, selanjutnya virus dengan cepat menyebar ke seluruh bagian sistem komputer. Setelah sistem inti pengguna terinfeksi oleh virus, akan mempengaruhi kerja normal pengguna dalam waktu singkat, sehingga menyebabkan kerugian yang tak terhindarkan bagi pengguna.

d. Pintu Belakang dan Kebocoran Perangkat Lunak Komputer

Tidak ada perangkat lunak di dunia yang sempurna, sehingga banyak peretas suka memilih peranti lunak untuk diserang. Disebut "backdoor" berarti programmer meninggalkan pintu untuk di awal perancangan perangkat lunak, sehingga turut "memfasilitasi" operasi masa depan mereka. Backdoor semacam itu jelas bukan karena programmer tidak cukup kompeten, akan tetapi karena justru terlalu kompeten untuk memikirkan cara yang tidak masuk akal tersebut. Singkatnya, perilaku tersebut adalah tidak masuk akal atau tidak direkomendasikan.

e. Sistem Serangan Langsung

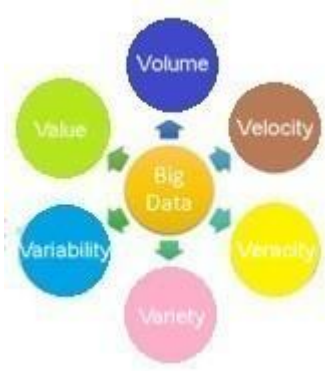
Dengan perkembangan ilmu pengetahuan dan teknologi, beberapa orang yang akrab dengan komputer langsung menyerang sistem komputer orang lain melalui jaringan komputer yang dimiliki. Jenis kejahatan ini muncul dengan pengembangan bidang komputer. Serangan secara langsung pada sistem ini lebih canggih, bahkan tanpa meninggalkan beberapa jejak [9]. Dengan mencuri privasi, menghancurkan informasi nyata dan menyebabkan masalah besar bagi orang lain. Karena sifatnya tidak terbatas dari jaringan komputer, para penjahat ini menjadi semakin dan semakin merajalela. Hanya dengan meluangkan an sedikit waktu dan energi, tetapi mereka mendapatkan keuntungan yang besar, sehingga timbul keinginan menjadi lebih kuat

e. Bencana Alam

Tidak peduli seberapa cerdas komputer itu, komputer hanyalah sebuah mesin, yang selalu lebih rendah daripada manusia. Karena itu, ada faktor eksternal lain yang akan berdampak besar pada keamanan komputer, yaitu bencana alam. Bencana alam yang dimaksud merujuk pada penyebab yang tidak dapat dikendalikan seperti perubahan kelembaban, suhu, gempa bumi atau gempa bumi yang menyebabkan tsunami, pemadaman listrik yang tiba-tiba atau kecelakaan asupan air komputer. Penyebab alami ini berada di luar kendali manusia dan tidak bisa sepenuhnya dihindari. Karena itu, jika ingin meningkatkan keamanan jaringan komputer, kita harus melakukannya mulai dari aspek lain.

2.3 Big Data

Big data dapat dideskripsikan sebagai volume tinggi, kecepatan tinggi, dan variasi tinggi informasi yang menuntut bentuk inovatif dari pemrosesan informasi untuk mendapatkan wawasan dan untuk pengambilan keputusan [10]. Biasanya, *big data* ditandai dengan 6 sifat, umumnya disebut sebagai 6V.



Gambar 1. 6V dari Big Data

6V, yang merupakan karakteristik dasar dari *big data*, secara umum. Namun, data diklasifikasikan sebagai *big data* selama memenuhi 3V pertama yaitu volume, kecepatan, variasi [11]. Teknologi big data dapat digambarkan sebagai alat atau teknologi yang digunakan untuk memproses data secara efisien yang telah diklasifikasikan sebagai data besar. Beberapa teknologi *big data* termasuk, Apache Hadoop [12], Apache Spark [13], Apache Storm [14], Apache Flink [15], Apache Cassandra [16], dan Apache

HBase [17]. Pada bagian di telah digambarkan karakteristik *big data*, yaitu 6V.

2.4 Big Data dan Masalah Keamanan dalam Organisasi

Studi sebelumnya telah mengidentifikasi kemungkinan masalah keamanan dan privasi dalam kaitannya dengan data besar [18], [19]. Sebagai contoh, kekhawatiran yang muncul dalam pengumpulan data sensitif dan pribadi oleh organisasi yang terkait dengan masalah privasi [20]. Namun, privasi data bukan satu-satunya masalah dalam hal keamanan *big data*. Suatu organisasi juga rentan terhadap ancaman keamanan lain dan serangan siber karena jangkauan data yang lebih luas yang dikumpulkan dan disimpan. Mekanisme keamanan dalam organisasi dengan kemampuan *big data* perlu dipasang dengan benar untuk menghindari pelanggaran keamanan yang tidak diinginkan seperti berbagi data dan informasi sensitif kepada pihak yang tidak diinginkan. Tanpa mekanisme keamanan yang efektif, itu dapat menimbulkan beberapa dampak pada organisasi, di antaranya adalah kerusakan reputasi dan kerugian finansial [21]. Lee [21] juga berpendapat bahwa "keamanan yang lemah menciptakan resistensi pengguna terhadap adopsi data besar". Ini resistensi terhadap solusi *big data* adopsi juga didukung oleh temuan survei yang dilakukan oleh beberapa riset pemasaran dan teknologi perusahaan konsultan. Secara konsisten, faktor keamanan dan privasi disebut sebagai salah satu faktor penghalang utama bagi Adopsi solusi *big data* dalam organisasi [22], [23].

3. SOLUSI

Bagian ini membahas beberapa solusi pencegahan terhadap kerentanan serta ancaman keamanan komputer yang diusulkan.

3.1 Tindakan Pencegahan terjadinya Ancaman terhadap Keamanan Komputer

Teknologi pertahanan virus adalah tindakan pencegahan penting untuk keamanan jaringan komputer. Kekuatan dari virus perlu diperhitungkan, kerusakan yang disebabkan oleh virus pada jaringan tidak bisa dihitung. Beberapa virus dapat diisolasi dari komputer melalui pertahanan efektif, tetapi beberapa virus yang lebih parah tidak dapat sepenuhnya dihilangkan melalui beberapa jaring pelindung. Teknologi komputer terus diperbarui dan dikembangkan, tetapi peretas dan penjahat juga terus-menerus belajar, jadi kita tidak boleh berhenti mempelajari perkembangan jaringan komputer teknologi keamanan. Teknologi pelindung harus lebih cepat daripada kecepatan para penjahat komputer mempelajari virus.

Teknologi Enkripsi Data, seperti disebutkan sebelumnya, lubang keamanan informasi adalah salah satu masalah yang paling sering disebutkan dalam jaringan komputer keamanan. Dengan menggunakan teknologi enkripsi data, maka informasi pengguna tidak mudah dicuri. Enkripsi data merupakan teknologi yang mengacu pada penggunaan teknologi pemrosesan data khusus untuk menyembunyikan atau mengkhususkan data, yang melaluinya jaringan komputer, pengguna mungkin tidak memahami informasinya. Enkripsi data dapat dibagi menjadi dua bentuk: enkripsi kunci publik dan enkripsi kunci pribadi. Enkripsi kunci publik lebih aman daripada enkripsi kunci pribadi, dan itu berkembang relative terlambat. Enkripsi kunci pribadi dapat dibagi menjadi dua proses: enkripsi dan dekripsi. Enkripsi dan proses dekripsi berhubungan satu sama lain, yang memiliki efek perlindungan tertentu pada keamanan informasi. Enkripsi kunci pribadi tidak dibatasi oleh pengguna, siapa pun dapat mengatur dan menggunakannya. Dalam hal kecepatan dekripsi, enkripsi kunci lebih cepat daripada enkripsi kunci publik dan lebih mudah diterapkan dalam kehidupan. Membandingkan karakteristik kriptografi kunci publik dan kriptografi kunci pribadi, dengan menemukan bahwa memiliki kelebihannya sendiri. Secara private, jika enkripsi public key dan enkripsi private key dapat digunakan bersama-sama, efek enkripsi data harus lebih tinggi.

3.2 Kontrol Akses dan Teknologi Firewall

Kontrol akses merupakan fitur paling penting dari kontrol akses adalah untuk memverifikasi identitas pengguna yang mengakses sumber daya komputer. Dibutuhkan audit, verifikasi otorisasi, kata sandi, kunci, dan metode otentikasi lainnya untuk melindungi pengguna keamanan informasi dan komputer. Sederhananya, ide inti dari kontrol akses adalah bahwa informasi hanya terbuka pengguna yang benar-benar membutuhkannya, dan bahwa pengguna yang masuk secara ilegal dicegah. Kontrol akses merupakan sarana penting untuk melindungi keamanan jaringan komputer. Karena hal ini memiliki efek yang baik pada intrusi hacker.

Diharapkan bahwa akan ada perkembangan penelitian yang signifikan di masa yang datang.

Teknologi *Firewall*, *Firewall* merupakan teknik keamanan untuk melindungi keamanan komputer dan mencegah kegagalan komputer, juga termasuk jenis tindakan keamanan komputer yang paling umum digunakan. *Firewall* dapat berupa perangkat keras, perangkat lunak, atau antara dua komputer atau lebih. *Firewall* dapat memberikan peran yang lebih substantif dalam melindungi komputer, karena semua aliran data perlu disaring melalui *firewall* [24]. Secara umum, *firewall* memiliki fungsi berikut ini, fungsi pertama, firewall dapat mencegah orang lain yang tidak terkait memasuki komputer pribadi pengguna; fungsi kedua, bahkan jika seseorang dari luar memasuki sistem, maka *firewall* dapat mencegahnya mendekati fasilitas pertahanan; ketiga, *firewall* dapat mencegah mengunjungi situs khusus / tertentu karena kemampuannya memfilter alamat yang tidak dikehendaki; dan pada akhirnya, *firewall* dapat mencegah mengunjungi situs tertentu. Pada intinya komputer harus menyediakan pemantauan keamanan.

4. KESIMPULAN

Keamanan jaringan komputer adalah masalah yang harus diperhatikan oleh setiap pengguna komputer. Harus diperhatikan perlunya melakukan pembersihan situs-situs phishing, tautan ilegal, spam, dan sebagainya dalam komputer. Jangan pernah memberikan kesempatan kepada penjahat karena hal itu merupakan kelalaian yang bisa berdampak serius terhadap kemanan komputer. Selain itu, pengembangan teknologi keamanan jaringan komputer harus terus menerus dilakukan sesegera mungkin dan mengurangi elemen ilegal secara teknis. Masih ada jalan panjang yang harus ditempuh untuk perkembangan teknologi keamanan jaringan komputer dimasa depan. Berbagai terobosan teknis harus direalisasikan sebagai sesegera mungkin, dan langkah-langkah perlindungan keamanan juga harus ditingkatkan.

DAFTAR PUSTAKA

[1] S. Hu, "Analysis of hidden dangers of computer network security and discussion of preventive measures," *Inf. Comput. (theoretical Ed.*, vol. 11, pp. 159–158, 2010.

[2] F.-Z. B. Lahcen, "Big Data Security: Challenges, Recommendations and Solutions," in *Web Services: Concepts, Methodologies, Tools, and Applications*, 2015, pp. 301–313.

[3] S. Miele and R. Shockley, *Analytics : The real-world use of big data*. 2013.

[4] S. Sun, "Understanding the Factors Affecting the Organizational Adoption of Big Data," *J. Comput. Inf. Syst.*, vol. 0, pp. 1–11, 2016.

[5] A. Loukaka, "Discovering New Cyber Protection Approaches from a Security Professional Prospective," *Int. J. Comput. Networks Commun.*, vol. 9, pp. 13–25, 2017.

[6] B. Duncan, "Enterprise security and privacy: Why adding IoT and big data makes it so much more difficult," in *International Conference Engineering Technollogy, ICET 2017*, 2018, pp. 1–7.

[7] L. Goodendorf, "Managing Big Data," *Inf. Secur.*, vol. 4, pp. 29–33, 2013.

[8] L. Zhang, "Brief discussion on computer network security technology," *Comput. Knowl. Technol.*, pp. 45–46, 2006.

[9] T. Wang, "Brief analysis of computer network security problems and preventive measures," *Sci. Technol. Innov. Appl.*, vol. 2, p. 45, 2013.

[10] G. A, "Beyond the hype: Big data concepts, methods, and analytics," *Int. J. Inf. Manage.*, vol. 35 No. 2, pp. 137–144, 2015.

[11] A. K, "Bigdata: Issues, challenges, technologies and methods," in *Proceedings of the International Conference on Data Engineering*, 2019, pp. 541–550.

[12] V. K. Vavilapalli, "Apache hadoop yarn: Yet another resource negotiator," in *Proceedings of the 4th annual Symposium on Cloud Computing*, 2013, p. 5.

[13] M. Zaharia, "Apache spark: a unified engine for big data processing," *Commun. ACM*, vol. 59, no. ACM, pp. 56–65, 2016.

[14] van der V. J. S, "Dynamically scaling apache storm for the analysis of streaming data," in *IEEE First International Conference on Big Data Computing Service and Applications*, 2015, pp. 154–161.

[15] P. Carbone, "Apache flink: Stream and batch processing in a single engine," *Bull. IEEE Comput. Soc. Tech. Comm. Data Eng.*, vol. 36, p. 4, 2015.

[16] C. A, "A big data modeling methodology for apache cassandra," *IEEE Int. Congr. Big Data*, no. IEEE, pp. 238–245, 2015.

[17] B. D, "Proceedings of the 2011 ACM SIGMOD International Conference on Management of data," in *Apache hadoop*

goes realtime at facebook, 2011, pp. 1071–1080.

[18] B. Saraladevi, "Big data and Hadoop-A study in security perspective," in *Procedia Computer Sciences*, 2015, pp. 596–601.

[19] A. Sharif, "Current security threats and prevention measures relating to cloud services, Hadoop concurrent processing, and big data," in *International Conference Big Data, IEEE Big Data 2015*, 2015, pp. 1865–1870.

[20] B. Mennecke, "Privacy in the Age of Big Data : The Challenges and Opportunities for Privacy Research," in *Thirty Fifth International Conference Information System*, 2014, pp. 1–5.

[21] I. Lee, "Big data: Dimensions, evolution, impacts, and challenges," *Bus. Horiz*, vol. 60, no. 3, pp. 293–303, 2017.

[22] G. Inc, *Survey Analysis : Big Data Investment Grows but Deployments Remain Scarce in 2014*. 2014.

[23] S. Institute, *Enabling Big Data by Removing Security and Compliance Barriers*. 2015.

[24] C. Xu, "Computer network security and data integrity technology," in *Beijing: Electronic Industry Press*, 2005, pp. 11–13.