# ENCRYPTION SECURITY SHARING DATA CLOUD COMPUTING BY USING AES ALGORITHM: A SYSTEMATIC REVIEW

**Taufik Hidayat**[1]
[1] Teknik Komputer, Fakultas Teknik, Universitas Wiralodra
[1]gueopik@gmail.com

## ABSTRAK

Teknologi *cloud computing* merupakan revolusi yang dapat berbagi sumber daya, layanan dan data di antara pengguna melalui jaringan. Karena jutaan pengguna menggunakan hak yang sama pada jaringan untuk mentransfer data, maka data menjadi lebih rentan terhadap serangan keamanan dari pihak yang tidak memiliki hak akses atau penyusup. Sistem untuk keamanan data sekarang berkonsentrasi pada penyediaan keamanan internet dalam penyimpanan data *cloud*, tetapi kurang memperhatikan terhadap keamanan data saat sedang melakukan transfer data. Mempertimbangkan keamanan sebagai masalah yang sangat berpengaruh, sistem yang diusulkan berkonsentrasi pada penyediaan keamanan untuk mentransfer data menggunakan teknik enkripsi. Penelitian yang dilakukan menunjukkan bahwa pendekatan yang diusulkan meningkatkan keamanan sistem secara keseluruhan membuat penyusup sulit untuk mengambil data yang di transfer. Untuk mencegah itu semua penulis mengusulkan metode enkripsi pada *cloud computing*dengan menggunakan algoritma AES (*Advanced Encryption Standard*) yang dapat melakukan proses pengamanan dalam proses transfer data maupun penyimpanan data. Metode yang dilakukan dalam mencari usulan penelitian menggunakan sistematika *review*, karena metode SLR mampu berikan usulan dan peluang bagi penelitian pada masa mendatang.

**Kata Kunci:***cloud computing, encryption, data sharing, algorithm AES*

## *ABSTRACT*

*Technology cloud computing is the revolution can share resources, services and data between users through a network of. Because millions of users use the same rights on the network to transfer data, and data to a vulnerable to attack security of the do not have the right of access or an intruder. System for security of data now concentrate on the provision of security the internet in data storage, cloud but little regard on security data while data transfer consider security as a very influential, the proposed concentrate on providing security to transfer data using a technique encryption. Research conducted show that the approach proposed boost security whole system make an intruder difficult to take the data in the transfer. To prevent it proposes encryption writer methods in cloud computing with algorithm AES (Advanced Encryption Standard) the process of security in the process of data transfers and data storage. The method is in search of the research uses systematic review, because method SLR able to give suggestions and opportunities for research on the future.*

***Keyword:*** *cloud computing, encryption, data sharing, algorithm AES*

## I. PENDAHULUAN

*Cloud computing* merupakan sebuah layanan penyimapanan berbasis *cloud* atau berbasis internet. *Cloud computing* menyediakan layanan untuk penggunanya untuk melakukan penyimpanan terhadap data yang dimilik pengguna tersebut. Penggunaan layanan

P-ISSN: 2621-8070
E-ISSN: 2686-3219

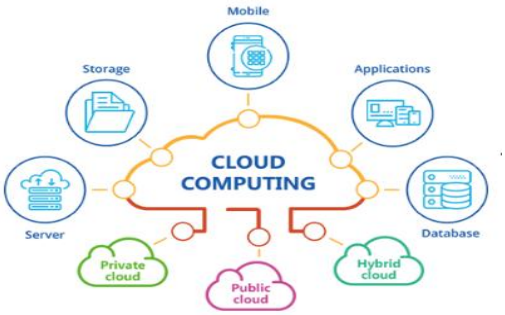
*cloud* menunjukkan peningkatan yang sangat drastis, karena layanannya yang sangat luas yang dapat menyediakan fasilitas yang sangat mudah di akses. Karena tingginya penggunaan layanan *cloud*, maka harus disiapkan untuk kemanan data pengguna *cloud*. Para penyedia layanan *cloud*harus menyediakan keamanan data yang aman untuk penggunanya agar menjadi perhatian yang sangat penting bagi penyedia layanan *cloud*. Sebuah model keamanan data *cloud* diusulkan untuk mengatasi para penyusup yang menembus dan mengambil data pengguna *cloud*[1].

Keamanan data dan informasi adalah tantangan keamanan yang paling utama pada layanan *cloud*. Mengenkripsi data dan informasi pengguna *cloud* merupakan cara untuk mengamankan data dan informasi pengguna *cloud*[2]. Untuk mencegah itu semua maka diusulkan sebuah metode yang dapat mengantisipasi terjadinya penyusup yang masuk kedalam sistem *cloud*yaitu dengan melakukan enkripsi[3].Algoritma enkripsi yang diusulkan melibatkan kriptografi simetris yang dimana kunci yang sama digunakan untuk enkripsi dan dekripsi[4]. Untuk memberikan kemanan selama proses transfer data maka digunakan algoritma AES[5]. Algortima ini dianggap lebih efisien dari pada algoritma yang lainnya. Keuntungan menggunakan algoritma AES yaitu algoritma ini dapat melakukan enkripsi untuk jumlah data yang besar dan mengkonsumsi sedikit dalam pelaksanaannya. Sehingga dengan menerapkan algoritma AES pada layanan *cloud computing* ini diharapkan dapat melakukan pengamanan terhadap data dari pengguna *cloud*[1].

## II. PENELITIAN TERKAIT

### A. *Cloud computing*

Revolusi dimana setiap individu dapat berbagi data dan sumber daya, sistem saat ini berkonsentrasi pada keamanan penyediaan data yang disimpan pada penyimpanan *cloud* akan tetapi kurangnya perhatian terhadap keamanan data yang saat itu sedang di transfer, sepeti pada Gambar 1.

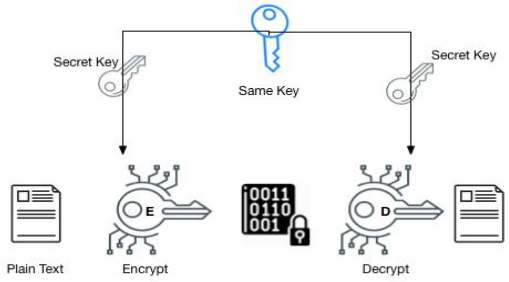



Gambar 1. *Cloud computing* [1]

*Cloud computing* menyediakan berbagai layanan seperti lingkungan pengembangan, alokasi dan relokasi sumber daya, penyimpanan dan kemampuan jaringan virtual dan lain lain [1]. *Cloud computing* dapat dinyatakan perangkat keras dan perangkat lunak sumber daya dan jasa yang ditawarkan melalui internet[6].

### B. *Algoritma Enkripsi*

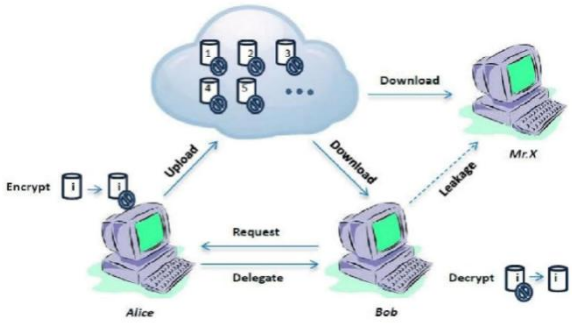
Sebuah model keamanan data *cloud* diusulkan untuk mengatasi penyusup masuk kedalam *cloud*. Selain kemanan data, enkripsi ini berkonsentrasi pada pada layanan penyediaan kemanan yang bertujuan untuk mentransfer data uang dikirimkan dengan menggunaan teknik enkripsi. Semua teknik berguna dalam enkrpsi realtime akan tetapi setiap masing-masing teknik memiliki caranya sendiri[1]. Seperti pada teknik enkripsi siaran sebagai penyumbang (ConBE) dimana sekelompok anggota menegosiasikan kunci enkripsi publik umum sementara masing-masing anggota memegang kunci dekripsi. Sebuah pengirim melihat kunci enkripsi sementara kelompok masyarakat dapat membatasi dekripsi untuk subset dari anggota pilihannya [6]. Algoritma enkripsi bisa dilihat pada Gambar 2.




Gambar 2. Algoritma Enkripsi [2]

### C. Data sharing

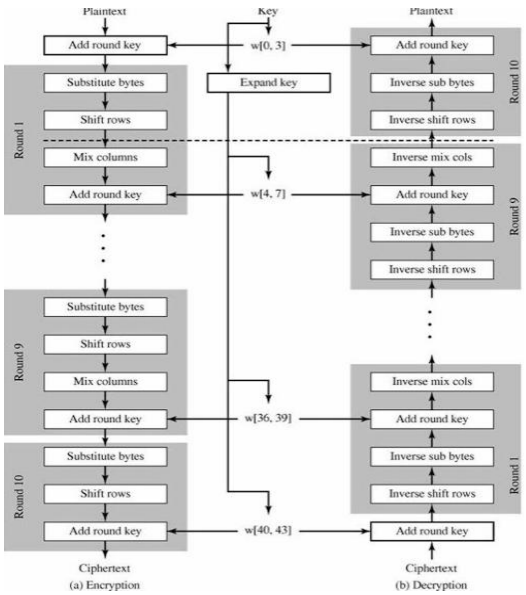
Data sebagai model layanan yang terkenal dimana data dan informasinya tersimpan di *cloud* yang disediakan untuk pelanggan dengan kebijakan akses mereka. Kemanan data dan informasi menjadi privasi yang membuat tantangan keamanan yang paling utama di *cloud* [2]. Hingga saat ini pengguna berbagi data pribadi, seperti foto dan video melalui aplikasi jejaring sosial berdasarkan penyimpnan *cloud* disetiap harinya. Namun, dengan menikmati kenyamanan layanan *data sharing* melalui penyimpanan *cloud* ini pengguna mengkhawatirkan tentang kebocoran data yang di sengaja pada penyimpanan *cloud*. Untuk mengatasi masalah kebocoran data pengguna ini pada penyimpanan *cloud*, maka dapat dilakukan pengenkripsian terhadap pemilik data yang semua datanya sebelum di upload pada penyimapanan *cloud*, sehingga pada akhirnya data di enkripsi dan dapat dapat dibuka oleh pemilik kunci tersebut [7]. Gambar *data sharing* pada Gambar 3.




Gambar 3. *Data sharing* [2]

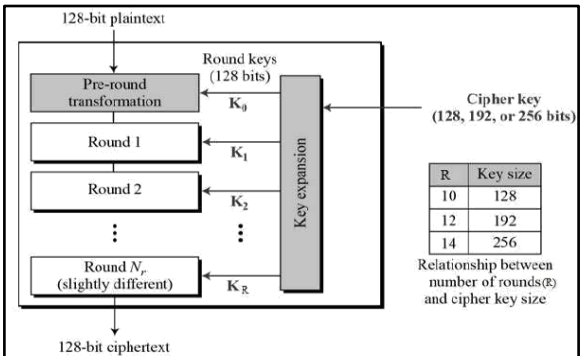
### D. AES Algoritma

AES telah banyak digunakan dalam berbagai sistem enkripsi seperti untuk keamanan data dan privasi [8]. Algoritma AES dipilih untuk melaukan enkripsi dengan alasan bahwa menggunakan algoritma ini lebih cepat dan lebih aman dibandingkan dengan algoritma IDES dan 3DES. AES dapat di definisikan sebagai simetris blok cipher yang merupakan salah satu proses enkripsi yang paling banyak digunakan. Semua operasi yang ada didalam algoritma AES dilakukan lebih dari 8-bit, cipher mengambil plaintext dari ukuran blok 128 bit, 192 bit dan 256 bit[9]. Kuncinya adalah digambarkan sebagai matriks persegi byte [10].




Gambar 4. Proses Enkripsi AES [6]

Algoritma AES mendukung panjang blok 128 bit dan ukuran kunci dari 128, 192 dan 256 bit. AES menggunakan seri 10 untuk kunci 128 bit, seri 12 untuk kunci 192 bit dan seri 14 untuk kunci 256 bit[11]. Pada masing-masing seri ini menggunakan kunci seri 128 bit yang berbeda, yang biasa dimaksud dengan kunci AES asli[1].

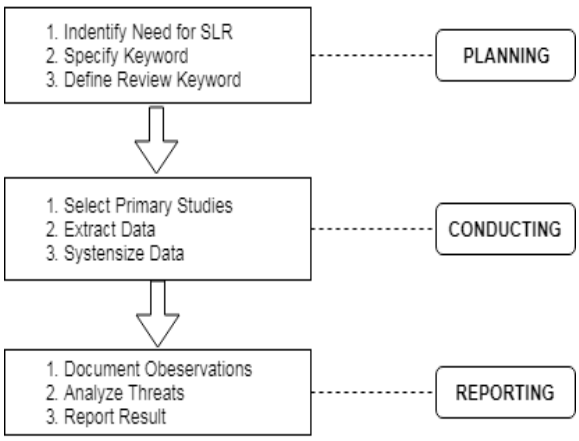



Gambar 5. Struktur Algoritma AES [1]

## III. METODE PENELITIAN

Pada Penelitian ini penulis mengunakan metode sistematika *review*, metode sistematika *review* merupakan metode formal dalam menilai serta menafsirkkan semua berkaitan dengan pertanyaan yang spesifik[12]. Sistematika *review* mempunyai tiga

tahapan[13]: merencanakan *review*, melakukan *review* dan melaporkan *review*[14]. Tahapan sistematika *review*seperti pada Gambar 6.




Gambar 6. Sistematika *Review*[14]

*A. Planning*

Tahap pertama merupakan perencanaan, tahapan ini bertujuan untuk mengindentifikasi tinjauan ulang mengenai sistematika dan menghasilkan *keyword*.

1. Mengidentifikasi kebutuhan SLR serta menentukan *keyword* yang sesuai dengan kebutuhan riset.
2. Menentukan *keyword* untuk mencari jurnal yang sesuai dengan tema.
3. Mengabungkan *keyword* yang satu dengan yang lain untuk mendapatkan jurnal yang spesifik serta mewakili tema yang akan di*review*.

*B. Conducting*

Tahapan kedua merupakan tahapan pemilihan jurnal dan hasilkan data yang diekstraksi dan informasi yang disintesis.

1. Memilih jurnal utama dari beberapa jurnal yang diperoleh dari *database* pencarian, kemudian seleksi jurnal yang berkaitan dengan SLR dan tema yang akan di*review*.
2. Pilih judul yang akan dibahas SLR, kemudian jurnal tersebut diektrak dengan mengambil abstrak dan kesimpulan.
3. Setelah jurnal diektrak kemudian dibuat sistematika *review* dengan cara menjelaskan apa yang telah dilakukan penelitian sebelumnya.

*C. Reporting*

Pada kesimpulan laporan, membahas *review* yang telah dilakukan oleh peneliti sebelumnya dan membandingkan apa yang membedakan dengan penelitian lain, SLR ini akan menghasilkan usulan baru dalam penelitian selanjutnya.

## IV. DISKUSI DAN HASIL REVIEW

Hasil *review* dalam bentuk *keyword* pencarian jurnal berdasarkan tema enkripsi terhadap data yang disimpan di*cloud*. Tahapanya sebagai berikut:

*A. Initiation and Identification of Review*

Penelitian ini menjawab permasalah dibidang enkripsi data pada bidang "*Cloud computing*", yang berkaitan dengan sharing data. Penulis tertarik untuk melakukan systematika *review* karena pengamanan pada *cloud computing* sangat perlu. Penulis mencoba melakukan pendekatan dengan menenukan tema terlebih dahulu dan menenteukan jurnal yang berkaitan degan tema.

*B. Data Sources for Selection*

Databse dalam pencarian jurnal penulis menggunakan dua sumber, yaitu "Science Direct" ditemukan www.sciencedirect.com, dan "IEEE Xplore" ditemukan www.ieeexplore.ieee.org. Pencarian dilakukan pada tanggal 30 Agustus 2019 dengan menggunakan *keyword* Security Data", "*Security Data sharing", "Security Data sharing Encryption", "Security Data sharing Encryption Storage", "Security Data sharing Encryption Storage Cloud computing", "Security Data sharing Encryption Storage Cloud computing with AES Algorithm*" semua *keyword* menggunakan huruf kecil tanpa tanda petik dan setiap kata dipisahkan spasi.

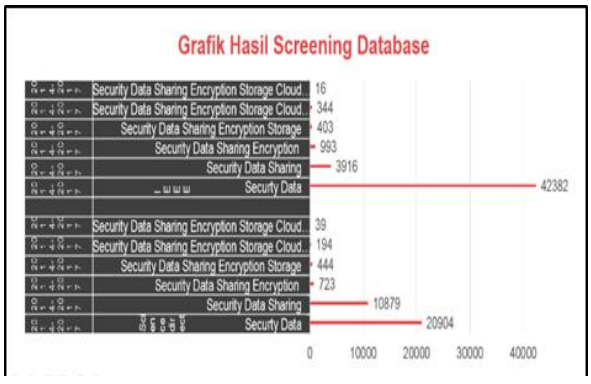
Pencarian jurnal dilakukan melalui 6 tahapan dengan kata kunci Q1" Security Data" lalu ditambah dengan kata kunci Q2" Security *Data sharing* "Q3 ditambah dengan kata kunci" Security *Data sharing* Encryption", Q4 ditambah dengan kata kunci" Security *Data sharing* Encryption Storage" Q5 ditambah

dengan kata kunci "Security *Data sharing* Encryption Storage *Cloud computing*". Dan kata kunci Q6 yaitu ditambahkan dengan "Security *Data sharing* Encryption Storage *Cloud computing* with Aes Algorithm". Pada tahapan pencarian jurnal penulis tidak mengunakan filter tertentu bertujuan untuk mendapatkan jurnal yang berhubungan dengan *keyword* yang ditulis, kemudian penulis menggunakan filter tahun dan jurnal untuk mempersempit pencarian.

Tabel 1. Hasil Pencarian Jurnal

| No. | *Database&Key words* | Hasil Jurnal | Tahun |
|---|---|---|---|
| 1. | **ScienceDirect** | | |
| | Q1 | 20904 | 2014-2019 |
| | Q2 | 10879 | 2014-2019 |
| | Q3 | 723 | 2014-2019 |
| | Q4 | 444 | 2014-2019 |
| | Q5 | 194 | 2014-2019 |
| | Q6 | 39 | 2014-2019 |
| 2. | **IEEE** | | |
| | Q1 | 42382 | 2014-2019 |
| | Q2 | 3196 | 2014-2019 |
| | Q3 | 993 | 2014-2019 |
| | Q4 | 403 | 2014-2019 |
| | Q5 | 344 | 2014-2019 |
| | Q6 | 16 | 2014-2019 |

Setelah melakukan pecarian maka didapat data seperti pada table 1, bahwa table 1 menunjukan penelitian yang membahas tentang *keyword* yang digunakan dalam systematika *review*, dari data pada table 1 maka dapat digambarkan secara grafik seperti pada Gambar 7.




Gambar 7. Grafik Hasil *Screening Database*

*C.* Analisis Reviw Jurnal

Dari *database* yang digunakan dengan *keywords* "Security *Data sharing* Encryption Storage *Cloud computing* with Aes Algorithm", bisa dilihat dari grafik pada gambar 7, bahwa *keywords* tersebut dapat menemukan judul yang terkait dengan systematic *review* yang penulis cari. Kemudian penulis mengambil jurnal dari kedua *database* sebanyak enam jurnal yang dianggap mendukung judul, selanjutnya penulis mencoba menganalisa dari jurnal tadi sebanyak tiga jurnal untuk dibandingkan dengan judul yang diangkat. Analisa jurnal dapat dilihat pada table 2.

Table 2. Analis Jurnal *Review*

| Paper | Penelitian Terkait | | | |
|---|---|---|---|---|
| | *Cloud* | Enkripsi | *Data sharing* | AES |
| [3] | x | x | v | x |
| [7] | v | v | v | x |
| [10] | v | v | x | v |
| Penulis | v | v | v | v |

Dari hasil systematika *review* bahwa penulis mencoba membandingkan pembahasan terkait tool dan metode yang dilakukan pada tiga tersebut. Bahwa dalam usulan penelitian dengan systematika *review* pada penggunaan algoritma AES untuk pengamanan *data sharing* pada *cloud computing* sangat perlu dilakukan, karena masih ada peluang untuk melakukan penelitian terkait penggunaan algoritma AES pada *cloud computing*.

## V. KESIMPULAN

Berdasarkan hasil pencarian string yang penulis lakukan, bahwa penerapan Algoritma AES untuk keamanan pada *data sharing cloud computing* masih banyak peluang untuk diimplementasikan, karena berdasarkan SLR yang telah dilakukan dari kedua database yang penulis himpun masih telalu sedikit orang membahasnya.Dari penelitian sebelumnya didapatkan bahwa penerapan security data pada *cloud* bisa berpengaruh terhadap keaslian data, serta bisa menghindari proses pencurian data oleh orang lain yang tidak memiliki izin untuk mengakses data tersebut. Metode systematika review mampu mendapatkan usulan penelitian selanjutnya yang belum dilakukan oleh para peneliti lainya dan memberikan kontribusi dalam bidang keilmuan baru yang akan dilakukan dimasa mendatang.

## VI. UCAPAN TERIMAKASIH

Penulis berterima kasih kepada fakultas teknik, Teknik Komputer Universitas Wiralodra yang memberikan motivasi untuk melakukan reseach.

## DAFTAR PUSTAKA

[1] K. M. Akhil, M. P. Kumar, and B. R. Pushpa, "Enhanced cloud data security using AES algorithm," *Proc. 2017 Int. Conf. Intell. Comput. Control. I2C2 2017*, vol. 2018–Janua, pp. 1–5, 2018.

[2] M. Hossain, R. Khan, S. Al Noor, and R. Hasan, "Jugo: A generic architecture for composite cloud as a service," *IEEE Int. Conf. Cloud Comput. CLOUD*, pp. 806–809, 2017.

[3] M. D. V. K. R. Boomija, "Secure data sharing through Additive Similarity based ElGamal like Encryption," *Int. Conf. Adv. Electr. Electron. Information, Commun. Bio-Informatics*, 2018.

[4] M. Joshi, K. Joshi, and T. Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems," *IEEE Int. Conf. Cloud Comput. CLOUD*, vol. 2018–July, pp. 932–935, 2018.

[5] L. Yu, D. Zhang, L. Wu, S. Xie, D. Su, and X. Wang, "AES Design Improvements Towards Information Security Considering Scan Attack," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 322–326, 2018.

[6] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farras, and J. A. Manjon, "Contributory broadcast encryption with efficient encryption and short ciphertexts," *IEEE Trans. Comput.*, vol. 65, no. 2, pp. 466–479, 2016.

[7] B. Cui, Z. Liu, and L. Wang, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2374–2385, 2016.

[8] Y. Yuan, Y. Yang, L. Wu, and X. Zhang, "A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation," *2018 IEEE Int. Conf. Electron Devices Solid State Circuits, EDSSC 2018*, pp. 4–5, 2018.

[9] V. Dilna and C. Babu, "Area optimized and high throughput AES algorithm based on permutation data scramble approach," *Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016*, pp. 3056–3060, 2016.

[10] A. Gupta and M. Jaiswal, "An Enhanced AES Algorithm Using Cascading Method On 400 Bits Key Size Used In Enhancing The Safety Of Next Generation Internet Of Things (IOT)," *Int. Conf. Comput. Commun. Autom.*, pp. 422–427, 2017.

[11] Y. Liu, W. Gong, and W. Fan, "Application of AES and RSA Hybrid Algorithm in E-mail," in *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, 2018, pp. 701–703.

[12] Fitroh and D. N. Utama, "Synthesizing a soft system methodology use in information systems research field: A systematic review," *2017 5th Int. Conf. Inf. Commun. Technol. ICoIC7 2017*, vol. 0, no. c, pp. 1–4, 2017.

[13] C. Soledad, "Methodology for Systematic Literature Review applied to Engineering and Education," *2018 IEEE Glob. Eng. Educ. Conf.*, pp. 1370–1379, 2018.

[14] P. Sharma and J. Singh, "Systematic literature review on software effort estimation using machine learning approaches," *Proc. - 2017 Int. Conf. Next Gener. Comput. Inf. Syst. ICNGCIS 2017*, pp. 54–57, 2018.