PENGENALAN POLA SERANGAN *BRUTE FORCE* PADA *CLOUD PUBLIC* DENGAN MENGGUNAKAN METODE *REGULAR EXPRESSION (REGEX)*

Oleh :

Yen Mey Sutedja
09011181621030

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

PENGENALAN POLA SERANGAN *BRUTE FORCE* PADA *CLOUD PUBLIC* DENGAN MENGGUNAKAN METODE *REGULAR EXPRESSION (REGEX)*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Yen Mey Sutedja
09011181621030

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2020

HALAMAN PENGESAHAN

PENGENALAN POLA SERANGAN *BRUTE FORCE* PADA *CLOUD PUBLIC* DENGAN MENGGUNAKAN METODE *REGULAR EXPRESSION (REGEX)*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

YFN MEY SUTEDJA
09011181621030

Inderalaya, Desember 2020

Mengetahui,

Pembimbing I

Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Pembimbing II

Ahmad Heryanto, S.Kom., M.T
NIP. 198701222015041002

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu
Tanggal : 23 Desember 2020

Tim Penguji :

1. Ketua : Ahmad Zarkasi,S.T., M.T
2. Sekretaris : Rendyansyah,S.Kom., MT
3. Anggota : Samayanta Sembiring, S.SI., M.T.

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Yen Mey Sutedja

NIM : 09011181621030

Judul : Pengenalan Pola Serangan *Brute Force* pada *Cloud Public* dengan Menggunakan Metode *Regular Expression* (Regex)

Hasil Pengecekan *Software iThenticate/Turnitin* :

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Inderalaya, Januari 2021

Yang menyatakan,

Yen Mey Sutedja

HALAMAN PERSEMBAHAN

"If you want good things, then you have to try to be good too. If you want to be happy, never forget the prayers and blessings of your parents. Because the blessing of parents is the blessing of Allah SWT"

"Skripsi ini saya persembahkan untuk kedua orang tua yang sangat saya sayangi dan juga keluarga besar dan tak lupa kepada orang-orang yang selalu menanyakan kapan " WISUDA " tanpa tahu proses dan hanya menilai dari hasilnya saja"

Segenap hati berterima kasih dengan

penuh rasa sayang kepada :

- *Ayah (Alirun) dan Ibu (Desi Ariska) tercinta*
- *Adik (Mega Lugita dan Al moza Bagus) tersayang*
- *Keluarga Besar Sistem Komputer Universitas Sriwijaya*
- *Civitas Akademika Universitas Sriwijaya*

KATA PENGANTAR

Puji syukur atas kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan judul **"Pengenalan Pola Serangan *Brute Force* pada *Cloud Public* dengan menggunakan Metode *Regular Expression (Regex)* "**.

Penulisan Proposal Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan proposal ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Orang Tua serta keluarga penulis tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan Tugas Akhir ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr.Ir.Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Deris Stiawan, M.T., Ph.D selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

5. Bapak Deris Stiawan, M.T., Ph.D selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Ahmad Heryanto, M.T. selaku Dosen Pembimbing II Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Samayanta Sembiring, S.SI.,M.T. selaku Dosen Penguji Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
10. Seluruh sahabat-sahabat saya, terkhusus Siti Aisyah, Fitriani, Ega Wahyu Ningsih, Widyana Aprianti,Diah Qomariah, Rofifah, Serly, Shabilla, Meri,Fitria Maharani dan Fitri Wulandari..
11. Almamater.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Proposal Tugas Akhir ini. Karena sesungguhnya tak ada yang sempurna didunia ini. Untuk itu, segala saran dan kritik sangatlah penting bagi penulis. Akhir kata, semoga Proposal Tugas Akhir ini dapat bermanfaat dan berguna bagi khalayak.

Palembang, Januari 2021
Penulis

Yen Mey Sutedja
NIM. 09011181621030

Introduction to Brute Force Attack Patterns on the Public Cloud Using the Regular Expression (Regex) Method

Yen Mey Sutedja (09011181621030)
Department of Computer Systems, Faculty of Computer Science,
Sriwijaya University
Email: yenmey.sutedja@gmail.com

Abstract

Brute Force is an attack carried out to crack passwords obtained from a set of passwords (wordlist) and will choose the right password to carry out such an attack. This research will present a regular expression method for an attack pattern. In the first step, the data will perform a data analysis manually by observing existing data, they will perform a rule experiment for an observed manual attack pattern. Then, it will be detected using the Snort Intrusion Detection System (IDS) to find out whether there is an attack in a public cloud. Furthermore, once detected, a separation of attack data or normal data will be carried out. In the last stage, pattern recognition will be carried out by using python coding using the regular expression (regex) method using the available rules in the extracted features. The dataset used in this study is the Brute Force Attack dataset. The proposed method allows for faster implementation and also achieves higher accuracy. In this case, the average value for the Brute Force A Attack dataset is 99% accuracy, 100% precision, 99% recall, and 100% f1 score. Compared to the DARPA 2000 dataset which only gets 91.5% accuracy. Based on these studies and results, it means that this method can be proposed and has higher accuracy in an attack pattern recognition study.

Keywords : Brute Force, Regular Expression (regex). Attack Patterns. DARPA 2000

Pengenalan Pola Serangan Brute Force pada Cloud Public dengan Menggunakan Metode Regular Expression (Regex)

Yen Mey Sutedja (09011181621030)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email : yenmey.sutedja@gmail.com

Abstrak

Brute Force adalah suatu serangan yang dilakukan untuk melakukan pembobolan *password* yang didapatkan dari kumpulan *password (wordlist)* dan akan memilih password yang tepat untuk melakukan suatu serangan tersebut. Dalam penelitian ini akan menyajikan metode regular expression untuk suatu pola serangan. Pada langkah pertama suatu data akan melakukan suatu analisa data secara manual dengan mengamati data yang ada, lalu akan melakukan suatu percobaan rule untuk suatu pola serangan manual yang telah diamati. Kemudian selanjutnya akan dideteksi menggunakan snort *Intrusion Detection System* (IDS) untuk mengetahui apakah terdapat suatu serangan didalam suatu *cloud public* tersebut. Selanjutnya setelah terdeteksi akan dilakukan suatu pemisahan data serangan ataupun data normal. Pada tahap terakhir akan dilakukan suatu pengenalan pola dengan cara menggunakan codingan *pyton* dengan menggunakan metode *regular expression (regex)* dengan menggunakan rule-rule yang tersedia didalam fitur-fitur hasil extraksi. Dataset yang digunakan pada penelitian ini adalah dataset *Brute Force Attack.* Metode yang diusulkan memungkinkan dapat mengimplementasi menjadi lebi cepat dan juga dapat mendapatkan akurasi yang lebih tinggi. Dalam hal tersebut didapat rata-rata nilai untuk dataset *Brute Force Attack* dengan Akurasi 99%, Precision 100%, Recall 99%, f1 Score 100%. Dibandingkan dengan dataset DARPA 2000 yang hanya mendapatkan Akurasi 91.5%. Berdasarkan penelitian dan hasil tersebut, berarti metode ini dapat diajukan dan mendapat keauratan akurasu lebih tinggi dalam suatu penelitian pengenalan pola serangan.

Kata Kunci : Brute Force, Regular Expression (regex), Pola Serangan, DARPA 2000

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Serangan *brute force* merupakan salah satu serangan yang menjadi ancaman bagi administrator layanan jaringan[1]. Serangan yang terjadi bertujuan untuk mendapatkan *username* dan *password* secara ilegal dengan cara mencoba semua kumpulan *username* dan *password* yang ada untuk mencoba masuk ke dalam suatu layanan jaringan. Suatu serangan dinyatakan berhasil jika terdapat kata yang cocok dalam kumpulan password yang telah tersedia.

NIST (*National Institute of Standards and Technology*), *Cloud Computing* adalah sebuah bentuk layanan yang membuka peluang untuk dapat diakses di manapun, memberikan kenyamanan, serta akses jaringan yang *on – demand* untuk penggunaan sumber daya komputasi terkonfigurasi [2].

Cloud computing mempunyai masalah kelemahan pada keamanannya, misalnya pembobolan *password* dengan menggunakan metode *brute force*. Dari uraian tersebut maka akan dilakukan serangan pada *cloud public* namun dengan metode yang sederhana menggunakan *regular expression* dengan mencoba semua *wordlist* yang tersedia.

Saat ini, *Utility Computing* bernama *Cloud Computing* yang telah berkembang pesat mengubah dinamika konsumsi TI melalui model yang menyediakan layanan *on-demand* melalui Internet ke banyak pengguna sekaligus [1]. Dalam perkembangan zaman server tradisional sudah mulai dialihkan pada *cloud ,* karena server tradisional membutuhkan biaya yang mahal dibandingkan dengan *cloud*. Maka dalam percobaan ini , lebih memilih cloud dibandingkan yang lainnya karena memiliki biaya yang lebih murah dibandingkan dengan lainnya.

Owncloud pada *cloud computing* merupakan pemodelan *cloud computing* yang memberikan lingkup yang lebih kecil untuk dapat memberikan layanan kepada pengguna tertentu pada sebuah perusahaan berskala enterprise [2].

Owncloud merupakan salah satu perangkat lunak berbagi berkas gratis (lisensi AGPL) dan bebas, menyediakan pengamanan yang baik, memiliki tata cara yang baik bagi pengguna aplikasi untuk membagi dan mengakses data yang.

Secara terintegrasi dengan perangkat teknologi informasi yang tujuannya mengamankan, melacak, dan melaporkan penggunaan data. Cara kerjanya cukup sederhana yaitu satu komputer yang digunakan sebagai server lokal dengan harddisk berkapasitas luas. Kemudian klien hanya mendapat akses untuk dapat menyimpan data di server owncloud. Mereka bisa menyimpan data, berbagi data dari komputer masing-masing.

Teknologi pada *Intrusion Detection System* (IDS) umumnya menggunakan metode *signature base* untuk mendeteksi suatu jenis serangan. Kelemahan metode ini adalah tidak dapat mendeteksi jenis serangan baru dengan *signature* yang tidak terdapat pada basis data, maka besar kemungkinan serangan tersebut akan berhasil menyusup pada sistem dan tidak terdeteksi oleh IDS [1]. Untuk mengatasi masalah kelemahan tersebut, perlu adanya metode baru yang dapat mengurangi kesalahan-kesalahan dalam mendeteksi *intrusi* tersebut.

Pada penelitian yang dilakukan pada dataset DARPA 2000 tentang serangan brute maka dilakukan berbagai macam metode yang telah di uji , maka didapatkan akurasi yang paling tinggi dengan menggunakan metode[3]NFS-FLES (Fuzzy Logic Expert System) dengan akurasi yang didapat 91.5%.

Pada penelitian tugas akhir ini akan melakukan pengenalan pola serangan pada cloud public dengan metode *regular expression* pada o*wncloud* untuk mendeteksi pola dari serangan *brute force*. Dengan kelebihan yang dimiliki diharapkan akan dapat mewujudkan akurasi yang tinggi daripada metode lain.

1.2 Tujuan

Adapun tujuan dari penulisan Proposal Tugas Akhir ini adalah sebagai berikut :

1. Menerapkan metode *regular expression* untuk menganalisa suatu data.
2. Mengetahui pola serangan *brute force* pada *cloud*.
3. Menjelaskan kronologi pola serangan pada *cloud.*

1.3. Manfaat

Adapun manfaat yang dapat diambil dari dilakukannya penelitian ini adalah :

1. Dapat mengetahui pola serangan *brute force* pada *cloud* .
2. Dapat menjelaskan kronologi serangan yang terjadi pada *cloud.*
3. Dapat memberikan pengetahuan tentang kelebihan dan kekurangan pada IDS dengan metode *regular expression.*
4. Memberikan informasi mengenai keakurasian metode.

1.4. Rumusan Masalah

Rumusan masalah dalam tugas akhir ini yaitu sebagai berikut :

1. Bagaimana serangan *brute force* terjadi dengan metode *regular expression?*
2. Bagaimana akurasi yang bisa didapatkan dari penerapan metode *regular expression* pada *cloud* ?

1.5. Batasan Masalah

Batasan masalah dalam tugas akhir ini yaitu sebagai berikut :

1. Penelitian yang dilakukan *cloud* bersifat publik.
2. Metode yang digunakan untuk menganalisa akurasi data adalah dengan menggunakan metode *regular expression (Regex).*
3. Sistem *snort* dapat membuktikan adanya serangan pada *cloud.*
4. Data yang di gunakan didapat dari server *cloud* dan penyerang.

1.6. Metodologi Penelitian

Penelitian ini akan melewati beberapa tahapan :

1. Tahap Pertama (Perumusan Masalah)

   Dalam tahap ini penulis menentukan permasalahan yang ada di *cloud computing* yaitu keamanan yang terjadi pada *cloud computing* untuk mengidentifikasi serangan yang terjadi dan membuktikan serangan tersebut.

2. Tahap Kedua (Studi Pustaka / Literatur)

Pada tahap ini penulis akan mencari informasi yang di perlukan melalui media pebelajaran sepert jurnal ilmiah, buku internet serta serta artikel-artikel terkait yang mendukung penulisan proposal tugas akhir ini.

3. Tahap Ketiga (Perancangan menggunakan metode *Regular Expression*)

Dalam tahap ini dilakukan perancangan sistem yang akan dibuat sesuai dengan rumusan masalah penelitian.Pada tahap ini akan melakukan instalasi *operation system* untuk mebangun jaringan *cloud* dan konfgurasi jaringan *cloud.*

4. Tahap Keempat (Pengujian)

Pada tahap ini dilakukan pengujian dari sistem yang dirancang. Ditahap ini seragan *brute force* akan diuji menggunakan linux ubuntu pada *cloud.*

5. Tahap Kelima (Analisis)

Pada tahap ini ialah tahap analisa dari hasil pengujian. Ditahap ini akan dianalisa bagaimana serangan itu dilakukan dengan bukti dan kronologis yang details.

6. Metode Analisa dan Kesimpulan

Hasil dari pengujian dari metode pengujian kemudian analisa dan dibuat saran sebagai referensi apabila penelitian ini dilanjutkan dan dibuat kesimpulan dari hasil penelitian.

1.7. Sistematika Penulisan

Untuk lebih memudahkan dalam menyusun tugas akhir ini dan memperjelas isi dari setiap bab yang ada pada laporan ini, maka dibuatlah sistematika penulisan sebagai berikut.

BAB I PENDAHULUAN

Pada bab I akan berisikan latar belakang masalah, tujuan, manfaat, perumusan masalah dan batasan masalah serta metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada Bab II akan berisi dasar teori *Brute Force Attack*, *Cloud Computing, Regular Expression, Snort* yang berkaitan dengan penelitian.

BAB III METODOLOGI

Pada Bab III akan membahas penjelasan secara bertahap mengenai proses penelitian yang dilakukan. Penjelasan tersebut meliputi tahapan perancangan sistem dan menerapkan metode penelitian.

BAB IV PENGUJIAN DAN ANALISA

Pada Bab IV menjelasakan mengenai hasil dari pengujian yang telah dilakukan selama penelitian tuhas akhir. Hasil dari pengujian itu akan dianalisi dari serangan *brute force* yang dilakukan *cloud.*

BAB V KESIMPULAN DAN SARAN

Pada bab V berisi kesimpulan akhir dari bab-bab pembahasan penelitian yang telah dilakukan dan juga berisi saran yang diperlukan untuk pengembangan penelitian selanjutnya.

DAFTAR PUSTAKA

[1] F. Durao, J. F. S. Carvalho, A. Fonseka, and V. C. Garcia, "A systematic review on cloud computing," *J. Supercomput.*, vol. 68, no. 3, pp. 1321–1346, 2014, doi: 10.1007/s11227-014-1089-x.

[2] H. Supendar and Y. Handrianto, "Teknik Owncloud Dalam Pengolahan Data Cloud Computing Berbasis Linux," vol. 5, no. 2, pp. 103–112, 2018.

[3] N. Liao, S. Tian, and T. Wang, "Network forensics based on fuzzy logic and expert system," *Comput. Commun.*, vol. 32, no. 17, pp. 1881–1892, 2009, doi: 10.1016/j.comcom.2009.07.013.

[4] R. Davidrajuh and C. Rong, "Solving Scheduling Problems with Randomized and Parallelized Brute-Force Approach," *12th Int. Conf. Comput. Sci. Inf. Technol. CSIT 2019*, pp. 1–4, 2019, doi: 10.1109/CSITechnol.2019.8895104.

[5] M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, "Machine learning for detecting brute force attacks at the network level," *Proc. - IEEE 14th Int. Conf. Bioinforma. Bioeng. BIBE 2014*, pp. 379–385, 2014, doi: 10.1109/BIBE.2014.73.

[6] D. Stiawan and S. Sandra, "Comparative Analysis of K-Means Method and Naïve Bayes Method for Brute Force Attack Visualization," 2017.

[7] M. Golasowski, J. Martinovič, and K. Slaninová, "Comparison of K -means Clustering Initialization Approaches with Brute-Force Initialization," pp. 103–114, doi: 10.1007/978-981-10-3409-1.

[8] M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert, and C. Kemp, "Detection of SSH brute force attacks using aggregated netflow data," *Proc. - 2015 IEEE 14th Int. Conf. Mach. Learn. Appl. ICMLA 2015*, pp. 283–288, 2016, doi: 10.1109/ICMLA.2015.20.

[9] J. K. Lee, S. J. Kim, C. Y. Park, T. Hong, and H. Chae, "Heavy-tailed distribution of the SSH Brute-force attack duration in a multi-user environment," *J. Korean Phys. Soc.*, vol. 69, no. 2, pp. 253–258, 2016, doi: 10.3938/jkps.69.253.

[10] P. Mell and T. Grance, “The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology,” *Public Cloud Comput. Secur. Priv. Guidel.*, pp. 97–101, 2012.

[11] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. Ullah Khan, “The rise of ‘big data’ on cloud computing: Review and open research issues,” *Inf. Syst.*, vol. 47, pp. 98–115, 2015, doi: 10.1016/j.is.2014.07.006.

[12] E. K. Dewi and P. Kasih, “Analisis log snort menggunakan network forensic,” vol. 02, pp. 72–79, 2017.

[13] E. Ophie and S. Teknik, “Aplikasi Algoritma String Matching dan Regex untuk Validasi Formulir,” 2014.

[14] A. Budiyanto, “Pengantar Cloud Computing,” p. 10, 2012.

[15] R. Andriani, E. S. Pramukantoro, and M. Data, “Pengembangan Sistem Visualisasi Access Log untuk Mengetahui Informasi Aktivitas Pengunjung pada Sebuah Website,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 6, pp. 2104–2112, 2018.

[16] I. E. N. Thompson, “Regular Expression Search Algorithm,” pp. 419–422.

[17] E. Ophie, “Aplikasi Algoritma String Matching dan Regex untuk Validasi Formulir,” 2014.

[18] L. L. P. Jaworski, “(12) United States Patent,” vol. 2, no. 12, 2005.

[19] R. K. Balan, B. P. Lee, K. R. R. Kumar, L. Jacob, W. K. G. Seah, and A. L. Ananda, “TCP HACK: A mechanism to improve performance over lossy links,” *Comput. Networks*, vol. 39, no. 4, pp. 347–361, 2002, doi: 10.1016/S1389-1286(01)00310-3.

[20] P. Kediri, E. K. Dewi, D. Harini, and N. Miftachurohmah, “SNORT IDS SEBAGAI TOOLS FORENSIK JARINGAN UNIVERSITAS NUSANTARA SNORT IDS SEBAGAI TOOLS FORENSIK JARINGAN UNIVERSITAS NUSANTARA PGRI KEDIRI,” no. February 2017, 2018.

[21] S. Chakrabarti, “Study of Snort-Based IDS,” no. Icwet, pp. 43–47, 2010.

[22] N. Khamphakdee, “Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection,” pp. 69–74, 2014.

[23] F. A. Masse and A. N. Hidayat, “PENERAPAN NETWORK INTRUSION

DETECTION SYSTEM MENGGUNAKAN SNORT BERBASIS," vol. 1, no. 2, pp. 1–16, 2015.

[24] J. Penelitian *et al.*, "Implementasi mobile syncing owncloud sebagai media storage menggunakan sistem operasi berbasis open source," vol. 5, no. 1, pp. 33–41, 2017.

[25] G. Al, "Extracting Potential Forensic Evidences from Cloud Client Device using own Cloud as a Case Study," *Int. J. Comput. Appl.*, vol. 132, no. 7, pp. 15–21, 2015, doi: 10.5120/ijca2015907482.

[26] S. Marwati, "No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title," جامعة -العلوم كلية - الاحيائية التقنيات قسم بغداد ،العا رق ا, vol. المجلد 49, no. للعلوم رقية ا الع المجلة, pp. 69–73, 2008.

[27] M. Roesch, M. Roesch, and S. Telecommunications, "S N O R T — L I G H T W E I G H T I N T R U S I O N Snort – Lightweight Intrusion Detection for Networks," 1999.

[28] B. Martini and K. R. Choo, "Cloud storage forensics : ownCloud as a case study," *Digit. Investig.*, vol. 10, no. 4, pp. 287–299, 2013, doi: 10.1016/j.diin.2013.08.005.