Pembuatan Sistem Autentikasi Antar Fog *Node* Berbasis *Skema Challenge-Response* Menggunakan Operasi *Bitwise* dan Aritmatika

Development of Authentication System Between Fog Nodes Based On Challenge-Response Scheme Using Bitwise and Arithmetic Operations

Muhammad Helmi Utomo, Favian Dewanta, Ridha Muldina Negara
Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
muhammadhelmiu@student.telkomuniversity.ac.id, **favian@telkomuniversity.ac.id**, **ridhanegara@telkomuniversity.ac.id**

Abstrak

Cloud computing merupakan sebuah istilah umum yang berhubungan dengan pengiriman menggunakan *hosted service* melalui internet. Cloud computing masih memiliki beberapa kekurangan yaitu *latency* dan *bandwidth* yang digunakan cukup tinggi. Oleh karena itu, fog computing dikembangkan sebagai teknologi penyempurna dari cloud computing. Fog membantu cloud dalam masalah memproses dan komputasi data secara lokal. Kemudian, data dikirimkan ke cloud yang membuat *resources* dan waktu yang digunakan lebih sedikit dibanding semua proses dibebankan kepada cloud. Tugas Akhir ini berfokus pada autentikasi antar fog *node* untuk mendukung migrasi mikroservis pada saat pengguna berpindah lokasi. Skema autentikasi yang dimaksud yaitu fog yang sudah pernah terhubung dengan pengguna akan mengirimkan sebuah *challenge* kepada fog yang baru. Untuk proses autentikasi penulis menggunakan dua tipe skema *challenge-response* yaitu operasi *bitwise* dan aritmatika. Dapat dilihat *delay* rata-rata saat terjadi proses verifikasi fog antara operasi *bitwise* dan aritmatika adalah sebesar 3,94 ms dan 3,53 ms. *Delay* rata-rata untuk proses validasi dari dua skema *challenge* adalah sebesar 0,393 ms dan 0,347 ms. Selisih antara *delay* total proses dari dua skema *challenge* adalah 0,46 ms dengan operasi aritmatika lebih cepat dibanding operasi *bitwise*. Pada proses agregasi, *delay* yang didapat sebesar 2,86 ms saat pengguna mulai terhubung dengan fog yang baru.

Kata kunci : *Cloud Computing*, *Fog Computing*, Autentikasi, Agregasi.

Abstract

Cloud computing is a general term related to transmission using hosted service over the internet. However, the cloud computing still has several shortcomings, namely the latency and bandwidth used are quite high. Then, fog computing is developed in order to solve those previous aforementioned. Fog assists the cloud by processing and computing data locally and then sends them to the cloud. As a consequence, resources and time spent are less than all processes charged to the cloud. This final project focuses on authentication between fog nodes for supporting microservices migration when user move to another location. For the authentication process, we use two challenge-response types operations, which are bitwise and arithmetic. In this this final project the average delay during verification process between bitwise and arithmetic is 3.94 ms and 3.53 ms. The average delay of validation process between the two operations schemes is 0.393 ms and 0.34 ms. The difference of total delay between the two operations schemes is 0.46 ms with operations arithmetic faster than the bitwise. In the aggregation process, the delay is 2.86 ms when the user starts to connect with the new fog.

Keywords: Cloud Computing, Fog Computing, Authentication, Aggregation.

1. Pendahuluan

Seiring dengan pesatnya perkembangan zaman, teknologi saat ini mengalami perkembangan menuju kemudahan. Kebutuhan dalam mengakses dan menyimpan data di internet semakin bertambah. Karena tuntutan itulah muncul teknologi jaringan yang bernama cloud computing. Cloud computing merupakan sebuah istilah umum yang berhubungan dengan pengiriman menggunakan *hosted service* melalui internet. Cloud computing menggunakan jaringan

dari *server* yang jauh dari pengguna, dibanding menggunakan *local server*. Tetapi, cloud computing masih memiliki beberapa kekurangan yaitu penggunaan *bandwidth* yang cukup tinggi. Dikarenakan data yang akan diproses dikirimkan keluar dari *firewall* yang berakibat perlunya *bandwidth* yang relatif cukup besar. Dari kelemahan tersebut, dikembangkanlah teknologi yang membantu kinerja dari cloud computing dalam memproses data yang ada yaitu fog computing [1].

Fog computing memberikan layanan dari cloud ke perangkat *edge* untuk menyediakan layanan data, komputasi, dan penyimpanan kepada *end user* secara lokal [1]. Fog computing membuat tiga jaringan arsitektur *user to fog to cloud* dalam aplikasi yang berjalan secara r*eal time.* Pengguna membutuhkan *latency rate* yang rendah dalam pertukaran data antara cloud melewati jaringan internet. Oleh karena itu fog computing memproses data yang didapat pada setiap *node* dari fog. Keuntungan dalam implementasi fog yang menutupi salah satu kekurangan dari *cloud* merupakan penggunaan dari *bandwidth* yang kecil, karena data yang diproses tidak keluar dari *local area network*. Dalam hal ini menjadikan data yang diproses lebih cepat serta memberikan *delay* yang relatif kecil [2].

Virtualisasi merupakan aspek penting dalam cloud sama seperti fog computing. Virtualisasi membuat sebuah cloud dan layanan fog sebagai *virtual environment* yang memungkinkan terjadinya *multi-tenancy* dan juga efisiensi sumber daya. Migrasi sebuah layanan antar *nodes* merupakan fitur utama yang memberikan peningkatan dalam fleksibilitas dan adaptasi. Layanan *handover* pada fog akan dilakukan pada dua kasus. Pertama, mendukung kasus yang membutuhkan perpindahan layanan antar fog untuk mendukung mobilitas pengguna. Kasus kedua adalah memungkinkan manajemen sumber daya yang dinamis dari sebuah layanan fog computing [3].

Autentikasi merupakan sebuah layanan keamanan utama pada suatu sistem keamanan, yang secara umum memverifikasi entitas tertentu. Autentikasi berbasis sertifikat merupakan skema autentikasi yang umumnya digunakan pada suatu aplikasi untuk memverifikasi identitas. Namun, penggunaan sertifikasi pada sistem dapat menyebabkan masalah tingginya *latency.* Dikarenakan sistem yang memiliki otoritas dalam pemeriksaan akan terbebani dengan menangani banyaknya permintaan verifikasi yang harus diproses [4].

Fog membutuhkan pemindahan data dikarenakan layanan yang tersedia pada fog merupakan turunan dari layanan pada cloud. Contoh layanannya seperti komputasi data dan penyimpanan data. Tetapi, fog memiliki cakupan wilayah yang lebih kecil dibanding dengan cloud. Jadi, pada saat pengguna berpindah tempat maka akan diluar jangkauan dari fog tersebut. maka diperlukannya pemindahan layanan yang ada untuk menyanggupi kebutuhan tersebut. Dalam hal ini setiap fog akan saling terhubung untuk pemindahan layanannya maka dibutuhkan sistem keamanan untuk mencegah adanya serangan. Maka dari itu penulis mengusulkan membuat Tugas Akhir mengenai autentikasi berbasis *challenge-response* operasi *bitwise* dan aritmatika yang diharapkan dapat meningkatkan tingkat keamanan dan mengurangi *delay* yang terjadi pada saat proses penyambungan dan agregasi antar fog.

2. Dasar Teori /Material dan Metodologi/perancangan

2.1 Fog Computing

Fog Computing merupakan sebuah gagasan teknologi baru yang dikenalkan oleh Cisco pada tahun 2010 sebagai metode dalam pengolahan, penyimpanan dan pengelolaan data antara *cloud* dengan pengguna [5]. Fog computing memiliki layanan pengolahan dan penyimpanan data lebih cepat dan sangat dekat dengan perangkat fisik dari pengguna. Tujuan dari fog computing bukan untuk menggantikan cloud melainkan memberikan layanan baru yang membuat penggunaan layanan cloud dapat diakses lebih dekat dengan pengguna [6].

2.2 Cloud Computing

Cloud computing merupakan sebuah istilah umum yang berhubungan dengan pengiriman menggunakan *hosted service* melalui internet. Cloud computing menggunakan jaringan dari *server* yang jauh dari pengguna, dibanding menggunakan *local server*. Cloud computing menggunakan *platform* secara virtual yang menyesuaikan *resources* dengan cara menyediakan perangkat keras, perangkat lunak, dan data yang di atur secara dinamis. Tujuan dibuatnya cloud computing yaitu untuk memindahkan *local computing* ke *platform service oriented* menggunakan *server cluster* dan juga penggunaan *database* pada *data center* [7].

2.3 Agregasi

Agregasi data merupakan sebuah proses penggabungan dan analisis data yang diterima melalui sensor *nodes*. Pada proses ini meningkatkan jumlah pemakaian pada jaringan dengan cara mengeliminasi data yang terbuang pada saat transmisi data [8]. Proses dari agregasi data yaitu dengan cara pengumpulan banyak informasi yang berkaitan digabungkan menjadi sebuah

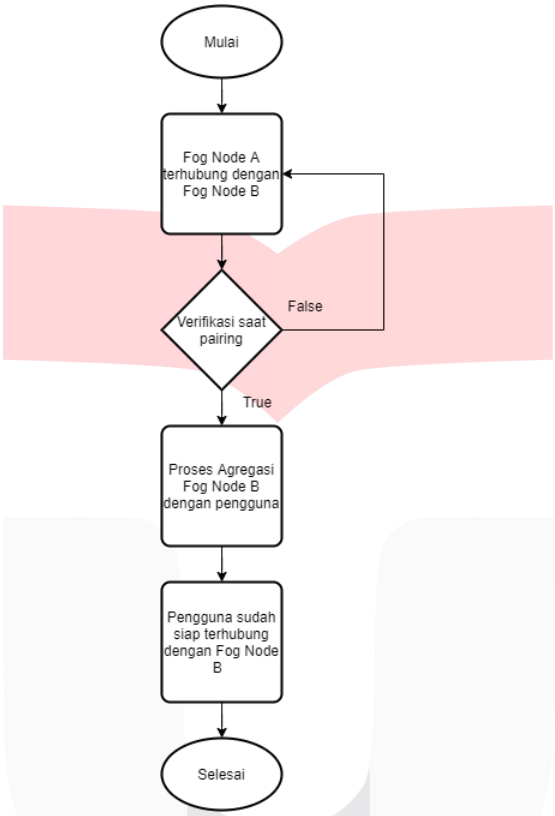
gabungan data yang besar dan informasi akan dikompres menjadi ukuran yang lebih kecil menggunakan fungsi dari agregasi data yang lain [9].

2.4 Zero Knowledge Proof

Zero Knowledge Proof adalah teknik dalam kriptografi menggunakan metode satu pengguna (*user*) membuktikan kepada pihak atau pengguna lain bahwa ia mengetahui nilai *x* tanpa mengungkapkan informasi selain fakta bahwa ia mengetahui nilai *x* tersebut. Secara singkat *Zero Knowlegde Proof* adalah metode untuk membuktikan kepemilikan tanpa mengungkapkan informasi itu sendiri atau informasi tambahan apapun [10].

3. Pembahasan

3.1. Desain Sistem



Gambar 1 Diagram Alir Sistem.

Tugas Akhir ini akan membangun sebuah virtualisasi sistem penyambungan antara fog A dan fog B dalam satu *local area network*. Penjelasan proses sistem pada gambar 1 adalah sebagai berikut.

1. Fog A terhubung dengan fog B.

   Sebelum terjadinya pemindahan layanan dari fog A ke fog B, kedua fog harus saling membangun koneksi awal menggunakan *socket programming* pada IP dan *port* yang sudah ditentukan sebelumnya dan melakukan proses autentikasi dari fog A ke fog B. Saat fog A mulai terhubung dengan fog B, fog A akan memberikan autentikasi berbasis *challenge-response* untuk memeriksa fog B *reliable* atau tidak.
2. Verifikasi saat sambungan antar fog.

   Untuk membuat koneksi awal dari fog A ke fog B dibutuhkan IP dan *port* yang sudah ditentukan. Dalam hal ini fog B memiliki ip 192.168.43.207, dan menggunakan port 8081. Setelah terkoneksi, fog A memberikan sebuah autentikasi yang berbasis yang berupa *challenge-response* operasi *bitwise* dan aritmatika kepada fog B untuk dijawab. Jika fog B sudah menjawab dengan benar dan fog A sudah memberikan respon dari jawaban yang diberikan maka fog B sudah terverifikasi sebagai *node* yang *reliable*.
3. Agregasi pengguna dengan fog B.

   Setelah terjadi perpindahan layanan dari fog A ke fog B, fog B memberi pemberitahuan kepada pengguna jika adanya penyesuain konfigurasi layanan dari fog A ke fog B kepada pengguna. Pengguna akan menunggu pesan dari fog B dan setelah menerima pesan, pengguna akan terhubung dengan fog B.

3.1.1 Skema Penyambungan

Pada skema penyambungan, terdapat 2 skema autentikasi yang akan digunakan yaitu operasi *bitwise* dan aritmatika.

- *Challenge* operasi *bitwise*.

```
root@ubuntu16-VirtualBox:/home/ubuntu16/final# python biner_fogA2.py
pemberian challenge response pada menit 24
maka masuk pada sesi 2
```

Gambar 2 Tampilan awal autentikasi untuk operasi *bitwise* pada fog A.

```
root@helmi-VirtualBox:/home/helmi/final# python biner_fogB.py
selesaikan  66 | 96?

jawabannya
98
```

Gambar 3 Tampilan awal autentikasi untuk operasi *bitwise* pada fog B.

Gambar 2 dan 3 merupakan autentikasi berbasis *challenge-response* operasi *bitwise*. Terdapat 3 sesi dalam waktu 1 jam, durasi masing-masing sesi 20 menit agar rendahnya probabilitas diberikan soal yang sama dari fog A. Sesi pertama, kedua, dan ketiga fog A akan memberikan tes berupa operasi gerbang logika secara berurutan AND, OR, dan XOR dengan kedua angka numerik yang dibuat secara acak dengan rentang dari 0 hingga 100.

- *Challenge* operasi aritmatika.

```
root@ubuntu16-VirtualBox:/home/ubuntu16/final# python aritmatika_fogA.py
pemberian challenge response pada menit 10
maka masuk pada sesi 1
```

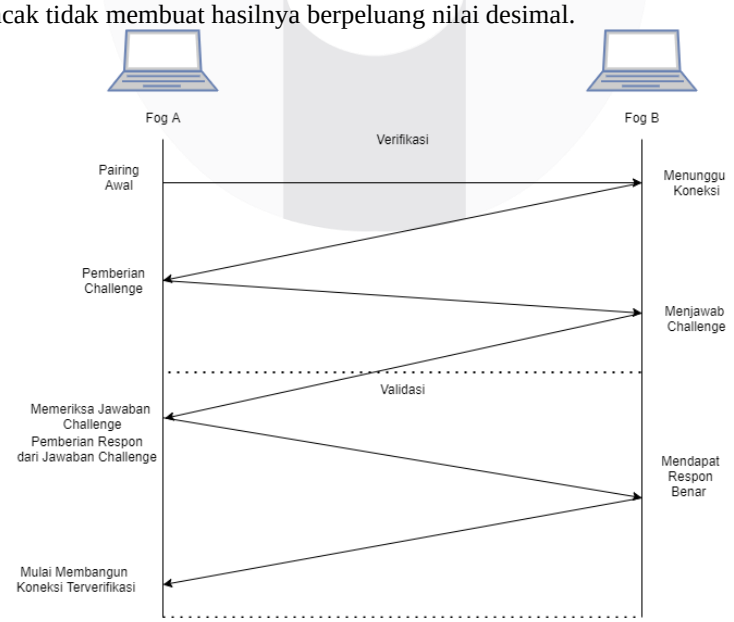
Gambar 4 Tampilan awal untuk operasi aritmatika pada fog A.

```
root@helmi-VirtualBox:/home/helmi/final# python aritmatika_fogB.py
berapa hasil operasi perhitungan  31 + 31?

jawabannya
62
```

Gambar 5 Tampilan awal untuk operasi aritmatika pada fog B.

Gambar 4 dan 5 merupakan autentikasi berbasis *challenge-response* operasi aritmatika hampir sama dengan *challenge-response* operasi *bitwise* sebelumnya, yang membedakan, pada *challenge* ini dibagi menjadi 4 sesi. Sesi pertama, kedua, ketiga, dan keempat fog A akan memberikan tes berupa operasi aritmatika yang secara berurutan penjumlahan, pengurangan, perkalian, dan sisa bagi. Penulis tidak menggunakan operasi pembagian agar kedua angka yang telah dibuat secara acak tidak membuat hasilnya berpeluang nilai desimal.



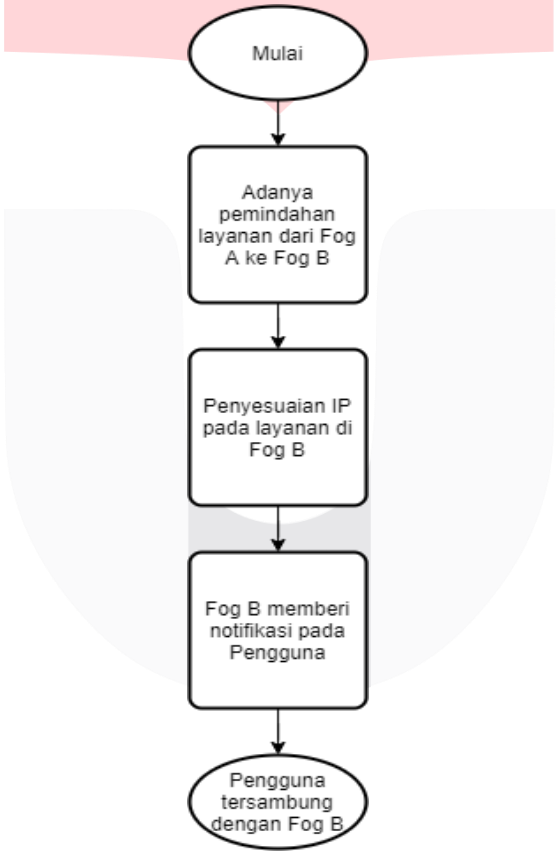
Gambar 6 Proses verifikasi dan validasi antar fog.

Gambar 6 menunjukan skema verifikasi dan validasi pada proses autentikasi yang digunakan penulis. Skema verifikasi yang dimaksud merupakan seperti dijelaskan di gambar saat

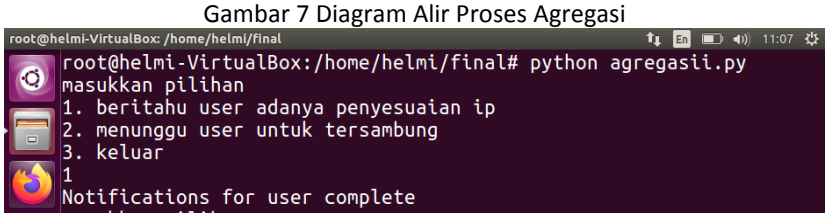
fog A melakukan pembangunan awal hubungan dengan fog B. Fog B dalam kondisi menunggu koneksi dari fog A. Ketika sudah tersambung, fog A akan memberikan sebuah *challenge* yang berisi operasi *bitwise* dan aritmatika. Setelah itu, fog B akan menjawab *challenge* yang dimaksud dan mengirimkan jawaban *challenge* ke fog A. Kemudian skema validasi yang dimaksud adalah saat fog A memeriksa jawaban *challenge* dan mengirim respon berdasarkan hasil pemeriksaan *challenge*. Jika jawaban *challenge* benar maka fog A akan mengirimkan respons kepada fog B jika jawaban dari *challenge* benar dan akan tersambung dengan fog A. Jika jawaban *challenge* salah maka fog A akan mengirimkan respons kepada fog B jika jawaban dari *challenge* salah dan gagal tersambung dengan fog A.

3.1.2 Skema Agregasi

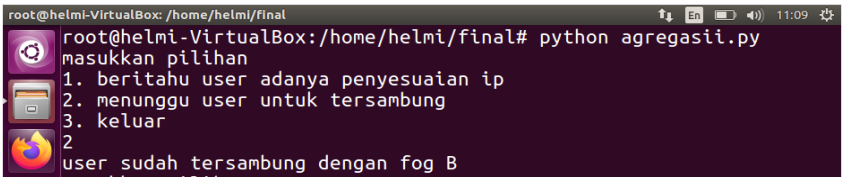
Setelah melalui proses autentikasi, proses pada skema agregasi dijelaskan melalui gambar 7 saat layanan sudah dapat di kirim menuju fog B. Saat fog B terjadi penyesuaian IP dari perpindahan layanan dari fog A, seperti pada gambar 8 terdapat pilihan awal yaitu fog B akan memberi tahu kepada pengguna bahwa adanya penyesuaian IP layanan dan menunggu pengguna memberi pesan kepada fog B bahwa pengguna siap terhubung.jika sudah terhubung maka akan seperti tampilan di gambar 9. Dapat dilihat dari gambar 10 setelah menerima pemberitahuan, pengguna membuka aplikasi yang sedang dalam posisi *standby* menekan tombol ‘OK’ untuk memberi tahu kembali kepada fog B. Saat pengguna menekan tombol ‘OK’ pengguna mengirim pesan kepada fog B bahwa pengguna sudah terhubung dan mengakses layanan pada fog.



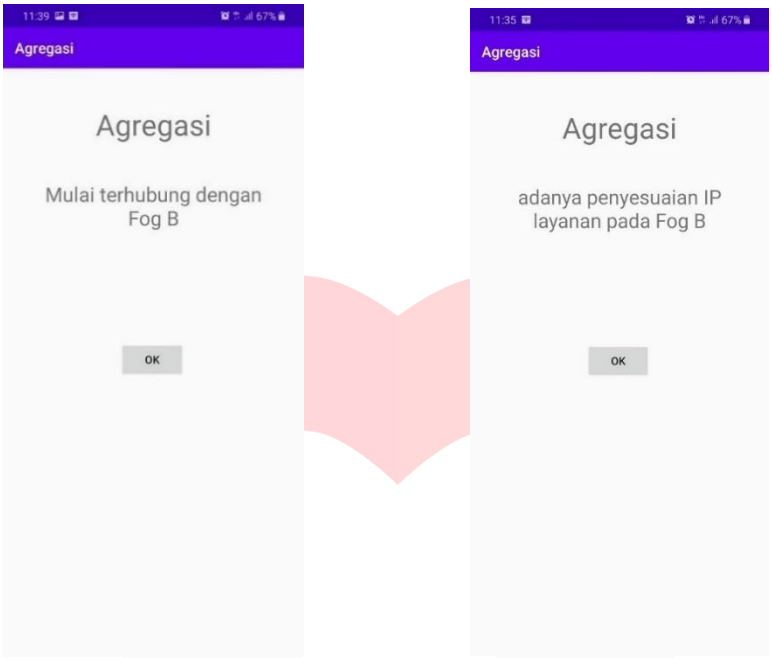
Gambar 7 Diagram Alir Proses Agregasi



Gambar 8 Tampilan awal dari fog B mengirim notifikasi kepada pengguna.



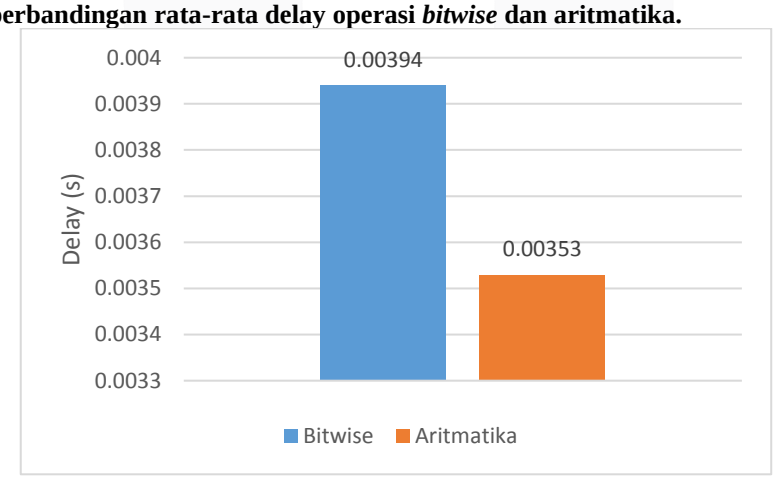
Gambar 9 tampilan pada fog B saat pengguna sudah tersambung.



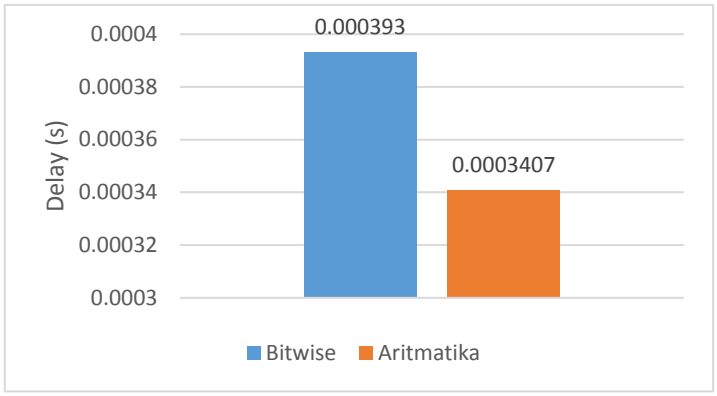
Gambar 10 Tampilan pengguna sebelum dan sesudah menekan tombol.

4. Hasil Dan Analisis

4.1.1 hasil perbandingan rata-rata delay operasi *bitwise* dan aritmatika.

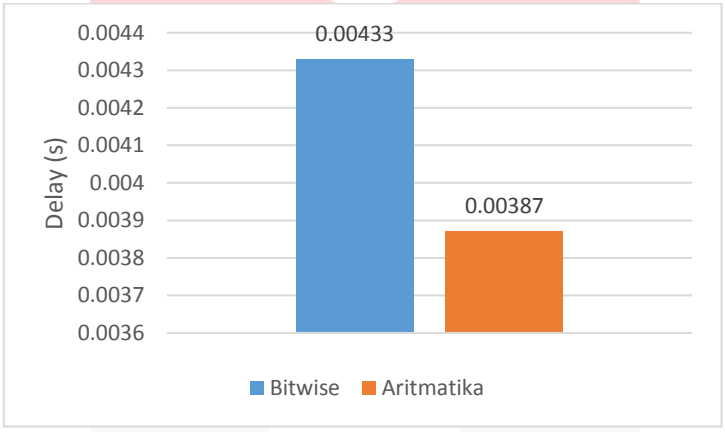


Gambar 11 Perbandingan rata rata *delay* saat verifikasi.



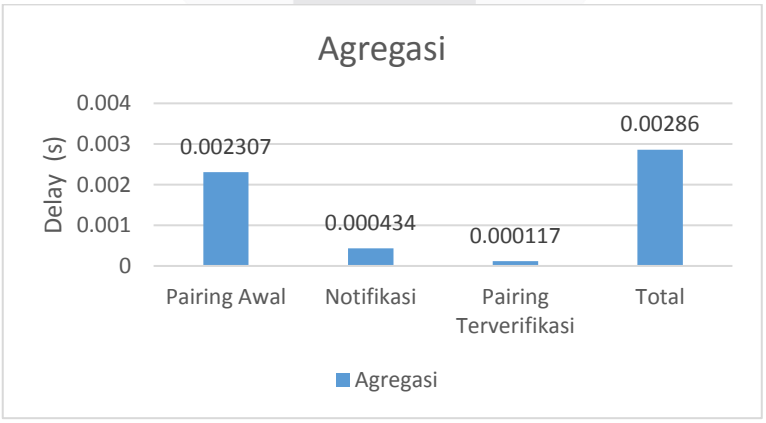
Gambar 12 Perbandingan rata -rata *delay* saat validasi.

Gambar 11 merupakan perbandingan hasil dari pengambilan 30 sampel rata-rata *delay* antara autentikasi berbasis *challenge-response* operasi *bitwise* pada saat proses verifikasi antar fog. Gambar 12 merupakan perbandingan rata-rata *delay* untuk proses validasi antar fog.



Gambar 13 Perbandingan rata-rata delay total proses.

Gambar 13 merupakan perbandingan rata-rata total proses menggunakan autentikasi untuk operasi *bitwise* dan aritmatika. Hasilnya *delay* untuk kedua autentikasi berbasis *challenge-response* memiliki rata rata *delay* masih dalam tahap yang cukup *reliable*. Tetapi adanya perbedaan total *delay* antara penggunaan *challenge-response* dapat berasal dari kemampuan tingkat komputasi dari perangkat yang digunakan sebagai fog. Dalam hal ini, dapat mempengaruhi variasi waktu *delay* proses yang terjadi. Tetapi *delay* pada kedua autentikasi masih termasuk dalam indeks yang sudah sangat baik.



Gambar 14 Grafik proses agregasi.

4.1.2 Rata-rata *Delay* Proses Agregasi

Gambar 14 sudah menjelaskan dan menunjukan seluruh proses dalam agregasi. Dapat dilihat rata-rata total *delay* yang didapat sebesar 2,86 ms dengan menggunakan *socket programming*

pada Python. Dalam hal ini dengan penggunaan *socket programming* pada agregasi, *delay* yang terjadi masih dalam tahap sangat baik.

5. Kesimpulan

Total waktu proses autentikasi untuk kedua skema yaitu operasi *bitwise* dan aritmatika memiliki rata-rata *delay* yang masuk dalam indeks yang sangat baik namun tidak terlalu jauh berbeda satu sama lain. Perbandingan proses antara autentikasi berbasis *challenge-response* operasi *bitwise* dan aritmatika untuk delay total pada operasi aritmatika lebih cepat 0.46 ms dibanding dengan operasi *bitwise*. Adanya perbedaan total *delay* antara penggunaan *challenge-respons*e dapat berasal dari kemampuan tingkat komputasi dari perangkat yang digunakan sebagai fog. Dalam hal ini, dapat mempengaruhi variasi *delay* proses yang terjadi. Penggunaan socket programming python pada agregasi masih dalam indeks *delay* yang sangat baik dengan *delay* total proses 2,86 ms. Disarankan menggunakan skema autentikasi lain dengan banyak fog dalam sekali autentikasi. Membuat eksperimen pemindahan layanan yang terjadi beserta penyesuaian konfigurasi pada layanan tersebut.

Daftar Pustaka:

[1] CISCO, "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are What You Will Learn," 2015.

[2] H. Wadhwa and R. Aron, "Fog Computing with the Integration of Internet of Things: Architecture, Applications and Future Directions," in *2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, 2018, pp. 987–994.

[3] C. Puliafito, C. Vallati, E. Mingozzi, G. Merlino, F. Longo, and A. Puliafito, "Container migration in the fog: A performance evaluation," *Sensors (Switzerland)*, vol. 19, no. 7, pp. 1–22, 2019.

[4] Y. Imine, D. E. Kouicem, A. Bouabdallah and L. Ahmed, "MASFOG: An Efficient Mutual Authentication Scheme for Fog Computing Architecture," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, 2018, pp. 608-613.

[5] F. Al-Doghman, Z. Chaczko, A. R. Ajayan, and R. Klempous, "A review on Fog Computing technology," *2016 IEEE Int. Conf. Syst. Man, Cybern. SMC 2016 - Conf. Proc.*, pp. 1525–1530, 2017.

[6] Z. Mahmood, Fog computing: Concepts, Frameworks and Technologies. Springer, 2018, doi: 10.1017/CBO9781316534298

[7] V. Soniya, H. Shaheen, R. Rangasamy, and T. Sreenivasulu, *Cloud Computing*, First Edit. Mumbai: VSRD Academic Publishing, 2018.

[8] H. Rahman, N. Ahmed, and M. I. Hussain, "A hybrid data aggregation scheme for provisioning Quality of Service (QoS) in Internet of Things (IoT)," *2016 Cloudification Internet Things, CIoT 2016*, pp. 1–5, 2017.

[9] S. Kaur and S. Sharma, "Performance evaluation based improved data communication with lossy links for wireless sensor networks," *2016 Int. Conf. Inf. Technol. InCITe 2016 - Next Gener. IT Summit Theme - Internet Things Connect your Worlds*, pp. 261–266, 2017.

[10] M. Harikrishnan and K. V. Lakshmy, "Secure Digital Service Payments using Zero Knowledge Proof in Distributed Network," *2019 5th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2019*, pp. 307–312, 2019.